Co-funded by
the European Union

CIVIL SOCIETY INITIATIVES
STRENGTHENED WITH
INFORMATION AND DATA SECURITY

PRACTICAL DIGITAL TRANSFORMATION GUIDE AND CURRICULUM ON STRENGTHENING DIGITAL SECURITY IN CIVIL SOCIETY

CIVIL SOCIETY INITIATIVES
STRENGTHENED WITH
INFORMATION AND DATA SECURITY

PRACTICAL DIGITAL TRANSFORMATION GUIDE AND CURRICULUM ON STRENGTHENING DIGITAL SECURITY IN CIVIL SOCIETY

CIVIL SOCIETY INITIATIVES STRENGTHENED WITH INFORMATION AND DATA SECURITY

PRACTICAL DIGITAL TRANSFORMATION GUIDE AND CURRICULUM ON STRENGTHENING DIGITAL SECURITY IN CIVIL SOCIETY

PRACTICAL DIGITAL TRANSFORMATION GUIDE AND CURRICULUM ON STRENGTHENING DIGITAL SECURITY IN CIVIL SOCIETY

Ankara, 2026

This study was conducted within the scope of the project titled “CIVIL SOCIETY INITIATIVES STRENGTHENED WITH INFORMATION AND DATA SECURITY” (2023-1-TR01-KA220-YOU-000161230), supported by the Turkish National Agency and the European Commission under the Erasmus+ Program. The content presented here reflects the views of the author, and neither the European Commission nor the Turkish National Agency can be held responsible for these views.

CIVIL SOCIETY INITIATIVES STRENGTHENED WITH INFORMATION AND DATA SECURITY

PRACTICAL DIGITAL TRANSFORMATION GUIDE AND CURRICULUM ON STRENGTHENING DIGITAL SECURITY IN CIVIL SOCIETY

SETA

SETA Publications 118
First Published in 2026 by SETA
E-ISBN: 978-625-5703-40-8

© 2026 SET Vakfı İktisadi İşletmesi All rights reserved.
No part of this book may be reprinted or reproduced or utilized in any form or by any electronic, mechanical or other means, without permission in writing from the publishers.

Academic Advisor: Erman Akıllı Cover Design and Layout: Erkan Söğüt & Said Demirtaş
Editorial Team: Ebrar Üzümcü, Sibel Koru, Zeyneb Güşta Arık, Sudib Sontoran Text Revisions: Cenay Babaoğlu
Date: Ankara, 2026
Printed in Türkiye, İstanbul by Turkuvaz Haberleşme ve Yayıncılık A.Ş.

SETA Publications
Nenehatun Caddesi No: 66 GOP Çankaya 06700 Ankara Türkiye Tel:+90 312.551 21 00 | Fax +90 312.551 21 90
www.setav.org | kitap@setav.org

In today's hyperconnected world, civil society organizations (CSOs), ranging from non-governmental organizations and advocacy groups to independent media outlets and community networks, operate on an increasingly complex digital front line. While digital tools have expanded the reach, efficiency, and impact of civil society, they have simultaneously exposed organizations to heightened cybersecurity risks. As civil society becomes more digitally dependent, it also becomes more digitally vulnerable.

Across Europe and beyond, CSOs are increasingly recognized as high-risk actors in the digital ecosystem. Cyberthreats targeting civil society now range from phishing, ransomware, spyware, and denial-of-service attacks to sophisticated state-sponsored surveillance aimed at silencing dissent and undermining democratic values. For organizations that often operate with limited technical capacity yet manage sensitive personal and organizational data, digital insecurity poses not only operational risks but also existential ones.

In this context, digital security is no longer a purely technical concern. It is mission-critical. The ability of civil society organizations to operate safely online is inseparable from their ability to protect freedom of expression, transparency, accountability, and the communities they serve. Strengthening digital security within civil society, therefore, requires more than ad hoc technical fixes. It demands structured learning, strategic planning, and practical guidance that can be implemented in real organizational settings.

Responding to this need, the KA220 Erasmus+ project "Civil Society Initiatives Strengthened with Information and Data Security" was initiated as a collaborative, multi-country effort to enhance the digital security capacity of civil society organizations. One of the central outcomes of this project is the present publication, which intentionally brings together two complementary functions in a single volume.

This book is designed as both a curriculum and a practical guidebook.

On the one hand, it functions as a structured digital security curriculum for civil society, offering a coherent learning pathway that builds knowledge

progressively – from understanding the digital threat landscape to developing organizational policies and incident response mechanisms. The curriculum-oriented structure makes it suitable for use in training, workshops, capacity-building programs, and train-the-trainer activities across different national contexts.

On the other hand, the book serves as a hands-on guidebook, providing concrete, actionable guidance that organizations can directly apply in their daily operations. Rather than remaining at the level of theory, it translates cybersecurity principles into practical steps, checklists, examples, and decision-making frameworks tailored to the realities of CSOs and grassroots initiatives operating with limited resources.

By combining these two dimensions, the book bridges a critical gap between learning and implementation. It allows readers not only to understand *why* digital security matters, but also *how* to operationalize it within their own organizations. Readers may approach the book sequentially as a curriculum, or selectively as a reference guide addressing specific challenges such as securing communications, protecting data, assessing risks, or building an internal culture of digital safety.

Written in an accessible yet academically grounded style, the publication draws on project-based experience, field insights, and established best practices in cybersecurity and civil society capacity building. Its modular structure enables adaptation to different organizational needs, technical levels, and national regulatory environments.

Ultimately, this combined curriculum and guidebook aims to empower civil society organizations to take ownership of their digital security. By fostering both knowledge and practical capability, it supports CSOs in strengthening their resilience, protecting their digital infrastructure, and continuing their essential work with greater confidence and sustainability in an increasingly contested digital space.

SETA, Ankara/Türkiye

1.1 PROJECT OBJECTIVE:

"Civil Society Initiatives Strengthened with Information and Data Security" is a KA220 Erasmus+ project coordinated by SETA (Türkiye) and implemented in cooperation with partner organizations from North Macedonia, Norway, Bosnia and Herzegovina, Belgium, and Türkiye. The project was funded by the European Commission through the Turkish National Agency and was designed to address the growing challenges faced by civil society organizations in an increasingly digitalized environment.

The primary objective of the project was to enhance digital literacy, cybersecurity awareness, and data protection capacities within civil society, while simultaneously promoting inclusion, diversity, and equal access to digital skills. Throughout its implementation, the project supported both individuals and institutions in navigating digital transformation processes and in strengthening their resilience against cyberthreats, misinformation, and disinformation.

Within this framework, the project produced a range of significant intellectual and practical outputs. These included a comprehensive **Digital Security Curriculum for Civil Society,** digital literacy and cybersecurity training modules, ensuring that digital transformation processes were accessible and inclusive. In addition, a **Practical Digital Transformation Guide** was developed to assist civil society organizations in planning, implementing, and sustaining effective digital transformation strategies.

Furthermore, the project developed a software-based **Online Digital Security Test Center for CSOs** to evaluate the cybersecurity readiness of civil society organizations. The platform enables CSOs to assess their digital security levels, including aspects such as data protection practices, system security configurations, and secure use of online tools (e.g., domain structures, HTTPS usage, and basic digital infrastructure safeguards). Through this tool, organizations are able to identify vulnerabilities, raise

awareness of existing risks, and support evidence-based capacity-building and improvement processes in digital security.

Beyond its educational outputs, the project also generated awareness-raising materials and campaigns focused on safe and responsible digital practices. Moreover, it succeeded in establishing a robust international cooperation network among partner countries, laying the foundation for long-term capacity building, knowledge exchange, and sustained collaboration in the field of digital security for civil society.

1.2 PROJECT PARTNERS:

FOUNDATION FOR POLITICAL, ECONOMIC, AND SOCIAL RESEARCH, SETA (COORDINATOR)

The Foundation for Political, Economic, and Social Research (SETA) is a non-profit think tank focused on producing accurate and up-to-date analyses on national, regional, and international issues. It aims to inform policymakers and the public on political, economic, social, and cultural developments within a historical and cultural context. As a research and policy-recommending institution, SETA fosters international dialogue, bringing diverse perspectives together through scholarly standards. It contributes to informed decision-making by government, civil society, and business leaders through research reports, publications, conferences, and policy recommendations. SETA adopts an interdisciplinary approach, recognizing the interdependence of political, economic, and socio-cultural issues, and seeks to promote a vision rooted in peace, justice, equality, and the rule of law. Its mission is to enrich strategic debates and provide independent, authoritative insights to decision-makers in both the public and private sectors.

FOUNDATION FOR POLITICAL, ECONOMIC, AND SOCIAL RESEARCH, SETA BRUSSELS

SETA Foundation for Political, Economic, and Social Research is a non-profit research institute focused on innovative studies related to national, regional, and international issues based in Brussels. Its objective is to produce accurate knowledge and analyses in politics, economy, and society, while informing policymakers and the public about evolving political,

economic, social, and cultural conditions. It fosters international dialogue by bringing diverse perspectives together through research reports, publications, conferences, and policy recommendations. The foundation aims to support informed decision-making in Türkiye by providing both public and private sector leaders with authoritative information and analysis. SETA's interdisciplinary research approach addresses the interdependence of political, economic, and socio-cultural issues, striving for a vision based on peace, justice, equality, and the rule of law.

ANKA FUTURE AND INNOVATION ASSOCIATION

ANKA is an innovative and dynamic non-governmental organization (NGO) based in Istanbul. Established in May 2019, it focuses on enhancing the mental, physical, and economic well-being of individuals by offering alternative sports activities, training, initiatives, and opportunities. ANKA aims to integrate technology and education, providing solutions that add value to individuals and society. The organization has expertise in mobile application development, artificial intelligence, web technologies, project management, and 3D modeling. Its members come from diverse professional backgrounds, including entrepreneurship, software, technology, health, and education. Additionally, ANKA organizes educational, cultural, and social activities to engage youth and foster active, healthy living. The organization strives to continuously develop its skills in the software sector

and contribute to lifelong learning processes through innovative technological solutions.

BOSNIAN REPRESENTATIVE ASSOCIATION FOR VALUABLE OPPORTUNITIES (BRAVO)

Bosnian Representative Association for Valuable Opportunities (BRAVO) is a dynamic NGO based in Bosnia and Herzegovina, focused on empowering individuals and communities through education, skill development, and capacity building. Its mission emphasizes social inclusion, cultural exchange, and sustainable development. BRAVO operates in various sectors, including youth empowerment, environmental awareness, entrepreneurship, and technology. It has a dedicated team of paid staff and volunteers who collaborate on numerous projects. BRAVO has organized youth exchange programs to promote cross- cultural understanding and personal growth, while also supporting environmental sustainability through innovative projects. It aids aspiring entrepreneurs with mentorship and resources, focusing on social impact. Additionally, BRAVO offers digital skills workshops, such as programming and web development, helping individuals enhance their personal and professional growth in technology.

TECHNOLOGY FOR TOMORROW'S BETTERMENT (TTB)

Technology for Tomorrow's Betterment (TTB) is a non-governmental organization based in Norway, dedicated to providing education and training in technology and digital skills to promote a sustainable future. Established on Oct. 6, 2019, by students in Trondheim, TTB aims to increase youth participation in the community by offering opportunities to gain knowledge and useful skills. With a team of 15 paid staff and numerous

volunteers, TTB implements projects in education, environment, and entrepreneurship. The organization focuses on digital innovation, youth work, and the integration of digital tools. Key activities include digital skills education, environmental initiatives, and supporting entrepreneurs, particularly in technology and sustainability. TTB values openness, collaboration, courage, and care, fostering a sustainable, ethical, and socially responsible environment. It engages in both regional and international cooperation.

TÜRKİYE YOUTH FOUNDATION (TÜGVA)

Founded in 2014, the Türkiye Youth Foundation (TÜGVA) is one of Türkiye's largest CSOs, with a team of over 100 professionals and 300,000 volunteers. It offers robotic coding workshops across 39 cities and manages 42 dormitories. The foundation operates with 10 coordinators in diverse fields, including sports, women's rights, entrepreneurship, media, education, culture, and career development. Its primary mission is to support the comprehensive development of youth, focusing on both physical and mental well-being, particularly in Türkiye. The foundation aims to empower young people to become innovative, productive, and valuable members of society. With more than 200 national and international projects completed, its vision is to cultivate generations capable of rebuilding and advancing civilization through continuous self-improvement and cultural enrichment.

ZDRUZENIE NA GRAGJANI MAKEDONSKA ASOCIJACIJA ZA COVECKI RESURSI SKOPJE (MHRA)

The Macedonian Human Resources Association (MHRA) is a non-profit, non-governmental national organization focused on workforce skills development, human capital promotion, and the standardization of informal education. MHRA's membership includes over 120 active individual

members, primarily women, and more than 600 passive members from the HR field, along with over 60 companies from both the public and private sectors. The association acts as an open platform integrating individuals at all career stages, including HR managers, consultants, employees, and students. It is involved in shaping policies related to business, education, and socio-economic issues at both national and local levels. An official member of the European Association for People Management (EAPM) since 2012, MHRA also embraces volunteering as a core value in its local and international initiatives.

TWO:

PRACTICAL DIGITAL TRANSFORMATION GUIDE FOR CSOS

2.1 CHAPTER

1: DIGITAL SECURITY FOR CSOS

What is Digital Security?

Digital security, also known as cybersecurity, is the practice of protecting digital information, devices, and other assets from unauthorized access or harm. It encompasses measures to safeguard personal data, accounts, files, and even financial resources stored or transmitted online. In essence, digital security aims to ensure the confidentiality, integrity, and availability of information (often summarized as the "CIA triad" – **C**onfidentiality, **I**ntegrity, **A**vailability).

Why is Digital Security Important?

In today's hyperconnected world, almost every organization and individual relies on digital systems. For CSOs and NGOs, this reliance includes communicating with stakeholders, managing donor information, and delivering services. Protecting these digital activities is critical. Cyberattacks can disrupt operations, breach sensitive data, and damage the trust that donors and communities place in an organization. For example, a data breach at the Australian Red Cross in 2016 exposed the personal information of over 550,000 blood donors due to a human error (an unsecured backup file). The incident not only raised questions about the organization's data practices but also led to a loss of donor confidence, illustrating how cyberincidents can harm real people and erode public trust in a CSO's mission.

Importantly, nonprofits are increasingly targeted by cybercriminals and even state-backed hackers. A Microsoft report found that humanitarian and human rights CSOs were the second most targeted sector by nation-state cyberattacks, accounting for 31% of such attack notifications in 2025. A

2023 study of Geneva-based nonprofits revealed 41% had experienced a cyberattack in recent years. Yet over half of those CSOs had no dedicated cybersecurity budget, and 70% felt they lacked the skills and resilience to respond to attacks. These figures underline that digital security is no longer optional but imperative for CSOs. Without adequate safeguards, cyberincidents can halt critical services, compromise beneficiary data, and jeopardize funding by damaging an organization's reputation.

Moreover, digital security is closely linked to physical safety and human rights in civil society work. Activists, journalists, and CSOs often face digital threats aimed at surveillance or intimidation. A breach or hack can expose sensitive communications or the identities of partners and beneficiaries, potentially putting lives or livelihoods at risk. Therefore, investing in digital security is investing in the overall resilience and trustworthiness of an organization's work.

What Does Digital Security Mean for CSOs?

For civil society organizations, *digital security* means protecting the information and technology that enable their social missions. The CSOs routinely collect and store sensitive data – from personal details of supporters and staff to strategic plans and research. Ensuring the confidentiality and integrity of this data is paramount so that it doesn't fall into the wrong hands or get tampered with. For instance, an advocacy group may need to secure contact lists of activists or evidence of human rights abuses. If such information were leaked or altered by malicious actors, it could endanger individuals or undermine the cause.

Digital security for CSOs also involves safeguarding daily operations. Many organizations rely on email, messaging apps, and cloud platforms to coordinate activities. If those accounts are compromised, attackers could disrupt communications or impersonate the CSO. In one real case, a charity's email system was hacked through a phishing email with a malware attachment, leading to a ransomware attack that encrypted the organization's server. The attackers demanded a ransom in exchange for the decryption key. Because the CSO had recent data backups and chose not to pay, they

were able to restore most of their data, yet about two weeks of information were permanently lost. This incident illustrates both the threat and the importance of preparedness: without strong backups and a response plan, the outcome could have been far worse.

For civil society groups that operate in sensitive political environments, digital security takes on an additional meaning of protecting the safety of their members and the communities they serve. Repressive entities may use cyber means to spy on CSOs or target them with disinformation. Thus, digital security for CSOs often emphasizes privacy-enhancing tools (like encryption for emails and messages) and safe communication channels to prevent surveillance. As Liberties, a European civil liberties organization, notes: CSOs using digital tools for activism face unique threats and must foster a culture of "digital self-defense" covering people, processes, and technology. In practical terms, this means training staff and volunteers on security awareness, establishing clear policies (for example, on handling personal data or using secure apps), and continuously updating technical protections.

Finally, *digital security for CSOs* is about sustaining trust. Donors and beneficiaries expect organizations to be good stewards of information. A well-publicized cyberincident can shake public confidence and deter people from engaging or contributing. For instance, after the Red Cross data leak mentioned earlier, the organization observed a decline in blood donations and had to work to rebuild trust. By prioritizing digital security, CSOs demonstrate their commitment to accountability and privacy, which are core values in the civil society sector.

Common Digital Threats and Risks to CSOs

CSOs face many of the same cyber risks as businesses and individuals, but often with fewer resources to address them. Some common threats include:

- **Hackers and Malware:** Attackers may try to infiltrate a CSO's network or devices to steal data or disrupt services. This can happen through malware (malicious software like viruses, spyware, or ransomware) delivered via email attachments, harmful links, or infected USB drives.

Ransomware is an especially damaging malware that encrypts files and demands payment. It has hit organizations of all sizes, from small nonprofits to entire city governments. If a CSO lacks strong anti-malware defenses and data backups, a ransomware attack could effectively paralyze its operations.

• **Phishing and Social Engineering:** Phishing is a tactic where attackers send fraudulent emails or messages that appear legitimate (for example, posing as a colleague or a service provider) to trick recipients into revealing passwords or downloading malware. Phishing is one of the most prevalent threats and often the entry point for larger attacks. CSOs have been targets of phishing scams; for instance, an education nonprofit nearly lost funding when attackers spoofed emails to trick a partner into sending a payment to the wrong bank account (a form of "business email compromise"). Common signs of phishing include urgent or alarming language, requests for sensitive information, or slightly misspelled email addresses. Social engineering can also occur via phone calls (vishing) or text messages (smishing) that impersonate trusted entities.

• **Data Breaches:** A data breach occurs when confidential information is accessed or disclosed without authorization. This can result from hacking, insider misuse, or even accidental exposure. CSOs often hold personal data (e.g., beneficiary details, donor financial records, health or legal case information) that are attractive to attackers or could be leaked. As mentioned, misconfigured servers or cloud storage can inadvertently leak data – the Red Cross incident being one example. The impact of a breach for a CSO is serious: it can lead to identity theft for individuals in the data, violate privacy laws, and damage the organization's reputation and legal standing. Unfortunately, many breaches trace back to human error. In fact, an industry report found that 74% of breaches involve a "human element," such as errors or falling victim to phishing. This highlights the need for training and careful handling of data.

• **Unauthorized Account Access:** Attackers may target the accounts that CSO staff use, such as email, social media, or fundraising platforms. By

stealing or guessing passwords (or using leaked credentials from previous breaches), they can hijack these accounts. Signs of compromise include login alerts from unfamiliar locations, new emails or posts sent that the user didn't create, or the inability to log in (password changed by an attacker). For example, if a CSO's official social media account is hacked, it could be used to spread false information or scam the CSO's followers. Using strong, unique passwords and two-factor authentication (discussed in Chapter 2) are key defenses against account takeovers.

- **Website Defacement or DDoS:** CSOs with public-facing websites could experience defacement (attackers altering the site's content to spread messages or propaganda) or Distributed Denial of Service (DDoS) attacks that flood the site with traffic to knock it offline. These attacks are sometimes carried out by hacktivists or opponents trying to silence a CSO's voice. One CSO discovered that their website had been redirected to a third-party site after attackers exploited vulnerabilities, and because they lacked a recent backup, it took nine months to rebuild their site. Ensuring website software is up-to-date and backed up can mitigate such risks.
- **Insider Threats and Human Error:** Not all risks come from anonymous hackers. Sometimes, insiders (employees or volunteers) can accidentally or intentionally cause security incidents. This could range from losing an unsecured laptop containing sensitive files to misconfiguring a database to a disgruntled staff member downloading data before departure. CSOs should be mindful of internal access controls and the principle of least privilege (giving staff access only to the information and systems necessary for their role). Moreover, fostering an organizational culture of security can reduce mistakes – when people understand why, for example, they shouldn't use personal USB drives or must follow data handling procedures, they are less likely to inadvertently create vulnerabilities.

In summary, CSOs face a broad array of digital threats – from everyday scams like phishing to more targeted attacks by sophisticated actors.

Chapter 2 will explore how to start guarding against these risks with basic best practices. But even at this introductory stage, one key point should be clear: recognizing the common risks is the first step toward managing them. By knowing what can go wrong (whether it's a stolen password, a virus infection, or a leaked document), organizations and individuals become more prepared to take action to prevent and respond to those scenarios.

What Will This Book Provide?

This guide is designed to equip civil society organizations with practical knowledge and skills to improve their digital security. It takes a straightforward, *hands-on approach* – similar to an open-university style course – with real examples, checklists, and simple exercises to reinforce learning. By going through the chapters, readers will:

- **Understand the Fundamentals:** You'll learn the terminology and core concepts of digital security (don't worry, we include a Glossary of Terms in the Appendix for quick reference). From basic definitions like what malware is to concepts like two-factor authentication, we'll demystify the jargon so you can communicate about security issues confidently.
- **Identify Your Risks:** The book will guide you through assessing what specific threats your CSO might face and what assets need protection. Through short self-assessment questions and scenarios, you will start mapping out your organization's risk profile (Chapter 3).
- **Implement Best Practices:** We provide clear, step-by-step advice on immediate actions – like how to create strong passwords, secure your devices, and safely use the internet and email (Chapter 2). These are the "quick wins" of cybersecurity that drastically reduce your vulnerability when done consistently.
- **Develop a Security Plan:** Beyond individual tips, we'll show you how to put it all together into a simple but effective digital security plan for your CSO (Chapter 3). This includes policy suggestions, training plans for your team, and methods for backing up and encrypting data. Templates and examples are provided to help you draft or improve your own plan.

- **Learn to Use Security Tools:** Chapter 4 introduces user-friendly security tools and software (from password managers and antivirus programs to secure messaging apps). We emphasize tools that are easy to use and commonly available, even on a small budget. Each tool or method discussed comes with an explanation of why it's useful and how to get started with it.
- **Prepare for Incidents:** Despite best efforts, incidents may happen. In Chapter 5, we walk through how to recognize signs of a cyberincident (like signs your computer might be hacked) and the immediate steps to take in response. Think of it as an emergency drill – knowing what to do can significantly limit the damage. We also list resources and contacts for getting help, because timely support can be crucial in a crisis.
- **Emphasize Collaboration:** A key theme in this guide is that you are not alone in tackling digital security. Chapter 6 discusses the power of peer support – how CSOs can help each other by sharing warnings, tips, and even pooling resources for training. It also points to networks and institutions (local or international) that offer support, from tech volunteers to helplines.
- **Provide Real-Life Context:** In Chapter 7, we present case studies and common pitfalls. You'll read brief stories of CSOs that faced cyber challenges and how they overcame them, as well as frequent mistakes organizations make (so you can avoid them). We also include a few simple exercises to "test" your security – for example, a checklist to audit your own office or a phishing email quiz for your team.

By the end of this e-book, you should feel more confident and empowered in dealing with digital security. The content is structured to be accessible even if you don't have an IT background. Each chapter builds on the previous ones, and you can also refer back to specific sections as needed. The goal is not to turn you into a cybersecurity expert overnight, but to give you the knowledge and habits that will significantly improve your protection against common threats. Think of it like a driver's manual for the digital

road – you don't need to be a mechanic to drive safely, but you do need to learn the rules, use the right tools (like seatbelts), and stay alert for hazards.

In addition, throughout the chapters, you will find "Did You Know?" side notes and short practice prompts to apply what you've learned. Take a moment to engage with these; they are there to solidify your understanding and make the learning experience more interactive. For instance, after the passwords section, a prompt might ask you to evaluate the strength of a sample password, or after the backup section, to consider what data in your organization is most critical to back up.

Ultimately, what this publication offers you is a foundation in digital security tailored for the civil society context. By investing time in these chapters, you are taking an important step toward safeguarding your organization's work and the people connected to it. So, let's begin the journey to a more secure digital future for your CSO!

Chapter Summary

This chapter introduces the critical importance of digital security for CSOs, highlighting their vulnerability as prime targets for cyberattacks due to their advocacy roles. It outlines common threats like malware, phishing, data breaches, unauthorized account access, website defacement, and DDoS attacks, emphasizing their impact on operations, trust, and safety. Real-world examples, such as the 2016 Australian Red Cross data breach, exposing 550,000 donors' information, and a ransomware attack on a charity, illustrate the consequences of inadequate defenses. The chapter notes that 31% of nation-state attacks in 2025 targeted CSOs, with 41% of Geneva-based nonprofits facing attacks, yet over half lack cybersecurity budgets. It stresses that digital security is mission-critical, protecting sensitive data (e.g., beneficiary details) and ensuring operational continuity. For CSOs in sensitive political environments, cybersecurity is linked to physical safety, preventing surveillance or disinformation. The chapter advocates for a culture of "digital self-defense," combining people, processes, and technology. It sets the stage for the e-book by framing cybersecurity as a survival necessity, not just an IT issue, and prepares readers for practical

solutions in subsequent chapters. Key takeaways include the need for awareness, preparedness, and trust-building to safeguard the CSOs' missions.

Quick Start Cybersecurity Checklist for CSOs

This checklist provides simple, immediate steps to enhance your organization's digital security. Complete these actions within the next week to reduce vulnerabilities and build a foundation for a secure digital environment. Each step is designed to be low-cost, user-friendly, and effective for CSOs with limited resources.

1. Secure Your Accounts

- Enable Two-Factor Authentication (2FA): Turn on 2FA for all critical accounts (e.g., email, social media, cloud storage) today. Use an authenticator app (like Google Authenticator or Authy) or SMS codes to add an extra layer of protection.
  - » Check account settings (e.g., Gmail: Settings > Security > 2-Step Verification).
- Create Strong, Unique Passwords: Update passwords for key accounts to be at least 14 characters, mixing letters, numbers, and symbols (e.g., "sunbird&glass7rain"). Use a different password for each account.
  - » Consider a free password manager like Bitwarden to generate and store passwords securely.
- Check for Breached Accounts: Visit "Have I Been Pwned" (haveibeenpwned.com) to see if your email or accounts have been exposed in data breaches. Change affected passwords immediately.
  - » Leaked credentials can be used to attack your accounts.

2. Protect Your Devices

- Update Software Today: Ensure all devices (computers, phones, tablets) and software (e.g., operating systems, browsers, apps) are updated with the latest security patches.
  - » Check Windows Update, macOS Software Update, or app store settings for pending updates.

• Install Antivirus Software: Install a free antivirus program (e.g., Windows Defender, Avast Free Antivirus) on all devices and ensure it's active and updated.

» Download from trusted sources and schedule weekly scans.

• Enable Device Lock: Set devices to auto-lock after five minutes of inactivity with a strong password or PIN. Ensure encryption is enabled (most modern devices have this by default).

» Locks and encryption prevent data theft if devices are lost or stolen.

3. Secure Communications

• Use Secure Messaging Apps: Switch to end-to-end encrypted apps like Signal or WhatsApp for sensitive communications. Verify contacts before sharing sensitive information.

» Download and enable disappearing messages for sensitive chats.

• Spot Phishing Emails: Train staff to avoid clicking links or sharing info in emails with urgent language, misspellings, or unfamiliar senders. Check email addresses carefully.

» Hover over links to verify URLs before clicking, and report suspicious emails to IT.

4. Safeguard Data

• Back Up Critical Data: Back up essential files (e.g., donor lists, project documents) to a secure external drive or cloud service (e.g., Google Drive with 2FA) this week.

» Schedule automatic backups or manually copy files to a secure location.

• Limit Data Access: Review who has access to sensitive data (e.g., shared drives, databases). Remove access for former staff or volunteers.

» Restricting access reduces the risk of insider threats or leaks.

5. Secure Your Online Presence

• Check Website Security: Verify your website uses HTTPS (look for the padlock in the browser). Contact your web host to ensure regular backups and updated software (e.g., CMS, plugins).

» Check with your hosting provider or use free tools like Let's Encrypt for HTTPS.

• Secure Social Media Accounts: Enable 2FA and strong passwords on all CSO social media accounts. Remove access for inactive admins.

» Protects against account hijacking and misinformation.

2.2 CHAPTER

2: FIRST STEPS IN DIGITAL SECURITY

First Steps in Digital Security

This chapter covers the fundamental practices that every individual in an organization should follow for basic digital safety. These "first steps" are often simple habits and measures that provide significant security benefits. As the saying goes, cybersecurity begins with cyberhygiene – the everyday routines and precautions that keep you safe online. We'll explore how to create strong passwords, use the internet cautiously, secure your communications, and protect your computers and smartphones. Even if you implement only these basics initially, you will already mitigate a large portion of common threats.

Creating and Protecting Strong Passwords

One of the most immediate ways to boost your digital security is to strengthen your passwords. Passwords are the keys to your accounts and devices – if they are weak or compromised, attackers can unlock everything from your email to your banking information. Unfortunately, people often reuse easy-to-remember passwords or choose ones that are easy for attackers to guess (like "123456" or "password"). In fact, weak or stolen passwords remain a leading cause of security breaches.

What is a strong password?

According to cybersecurity guidelines, a strong password is long, unique, and complex. Microsoft's security guidance suggests at least 14 characters, including a mix of upper- and lower-case letters, numbers, and symbols. It should **not** contain easy personal information (like your name or birthdate) or common words. A good practice is to use a *passphrase* – a series of

random words or a sentence that is easy for you to remember but hard for others to guess. For example, "sunbird&glass7rain" is far stronger than a short password like "blue123" yet might be easier to recall because it's a phrase.

Uniqueness is critical: each account or service should have its own password. If you reuse passwords and one account is breached, attackers will try that same password on your other accounts (a tactic called *credential stuffing*). Using unique passwords contains the damage of a single breach. As ENISA (the EU's cybersecurity agency) advises, *avoid using the same password on multiple accounts*. Also, consider checking if your accounts have appeared in known data breaches (websites like "Have I Been Pwned" allow you to search your email against breach databases). If so, change those passwords immediately.

Password managers: It's unrealistic to memorize dozens of long, complex passwords. That's where password manager tools come in. A password manager is an application (or secure cloud service) that can generate strong random passwords for you and store them in an encrypted vault, so you only have to remember one master password. Many security experts and agencies recommend using password managers for better security. For instance, Bitwarden (a password manager company) lauded ENISA's advice, which explicitly includes using a password manager to keep passwords unique and safe. Popular password managers include Bitwarden, LastPass, 1Password, and KeePass (among others). Find one that suits your organization (some have free versions) and start using it to upgrade all those weak or repeated passwords.

Protecting your passwords: Even a strong password must be protected. Never share your passwords over email or messaging, and be wary of anyone unsolicitedly asking for your password – legitimate support staff (even at IT companies) will not need your actual password. Also, enable Two-Factor Authentication (2FA) on your accounts whenever possible. 2FA (also called multi-factor authentication, MFA) means you provide a second proof of identity when logging in – for example, a one-time code sent to your phone

or generated by an authenticator app, or a fingerprint scan. This way, even if someone learns your password, they likely cannot access the account without that second factor. ENISA's top advice includes using "an extra step" like a phone code or biometric for logins. Many services (Google, Facebook, Microsoft, etc.) allow 2FA via an app or SMS. It's wise to turn this on for email accounts, social media, banking, cloud storage – essentially any account that would be sensitive if hacked.

Another important habit is to change default passwords on devices or applications. Many hardware devices (like Wi-Fi routers) or software tools come with preset admin passwords (often something generic like "admin/admin"). These defaults are widely known to attackers, so always set a new, strong password during setup. For example, if your CSO sets up a new office router or an online database, one of the first tasks should be customizing the access credentials.

Finally, consider a schedule for updating passwords periodically. Opinions vary on how frequently to change passwords – some experts say frequent forced changes can backfire (users might choose simpler passwords or just increment a number). Modern guidance suggests that if passwords are strong and unique, you need to change them only when there's an indication of compromise or periodically (say, once a year) as a refresh. The old rule of changing every three months is no longer a hard requirement if other controls (like 2FA) are in place. However, if you suspect any account might be compromised, change that password immediately, and anywhere else you used a similar one.

In summary, strong passwords + 2FA = a powerful defense. By using robust, distinct passwords and adding a second login step, you shut the door on many intrusion attempts. Think of it like locking your house with a high-quality lock (password) and a deadbolt (2FA) – an intruder would have to defeat both to break in. As a team, encourage everyone in your CSO to adopt these practices. Chapter 3 will touch on how to enforce good password policies organization-wide, but the change can start with you leading by example in using a password manager and 2FA for your accounts.

Safe Internet Use: What to Watch Out For

The internet is the main artery of information and communication for most organizations, but it can also be a source of threats if used carelessly. "Safe internet use" refers to practicing caution and smart behavior while browsing websites, using online services, and downloading content. Here are key principles and tips for CSO staff to follow:

***Verify Website Legitimacy*:** Before entering any sensitive information on a website (like login credentials or personal data), make sure the site is authentic and secure. Check that the URL is correct (watch for typos or strange domains that mimic real ones) and that the connection is encrypted – indicated by https:// and a padlock icon in the browser address bar. For example, https://secure.CSOportal.org is more trustworthy than http://CSO-portal.example.com (lack of HTTPS is a red flag). Attackers often create fake websites that look legitimate (for example, a site that impersonates an email login page) to phish passwords. Always double-check the address bar when logging in. Modern browsers also often highlight the company name in the certificate details for major sites – use those cues. When in doubt about a link received (say, via email or social media), do not click it directly. Instead, navigate to the official website via Google or bookmarks, or hover over the link to preview the URL (without clicking). If the link looks suspicious or doesn't match the purported sender (e.g., an email claims to be from your bank but the URL is some unrelated domain), it's likely malicious.

Think Before You Click or Download: Malicious links and downloads are a primary vehicle for malware. Be cautious when browsing unfamiliar sites or when prompted to download files. Pop-up windows that urge you to download a "codec" or "update" to view content are often traps. If you need a certain software or document, download it from a reputable source (for instance, software from the official vendor site or a well-known app store). Avoid downloading pirated software or media – aside from legal issues, such files frequently hide malware. Also, disable automatic downloads in your browser settings; having control means you can cancel anything unintentional. If your browser or security tool warns that a site might be

unsafe, heed the warning and leave the site. Similarly, be skeptical of browser extensions or plug-ins from unknown publishers. Only install add-ons you truly need and from official web stores, since a malicious extension could track your activity or inject ads/viruses.

Use Secure Connections (Wi-Fi and VPN): When connecting to the internet, especially outside the office, be aware of network security. Public Wi-Fi networks (like those in cafes, airports, etc.) can be risky because attackers on the same network might intercept your traffic. If you must use public Wi-Fi, avoid accessing sensitive accounts unless the connection is encrypted (look for HTTPS). Even then, a savvy attacker could set up a rogue Wi-Fi hot spot with a tempting name ("Free Airport WiFi") to lure users. A good practice is to use a VPN (Virtual Private Network) when on untrusted networks. A VPN creates an encrypted tunnel for all your internet traffic, which greatly reduces the chance of eavesdropping. Many organizations provide VPN access for remote work; if yours does, ensure you know how to use it. If not, consider using a reputable commercial VPN service when traveling or working from public spaces. Additionally, make sure your home or office Wi-Fi is secured with a strong password and is using WPA2 or WPA3 encryption. Change the default admin password on your router as mentioned and disable remote management unless absolutely needed.

Be Cautious with Email Attachments and Links: Although emails will be discussed more in the next section, it's worth noting as part of safe internet habits that clicking links in emails or on websites requires caution. A common scam online is fake alerts like "Your computer is infected! Click here to scan" – these often lead to malware. Similarly, avoid clicking on banner ads or pop-ups claiming you won something or that you need an urgent update. These are social engineering attempts to prey on curiosity or fear. Keep in mind the adage: if something online sounds too good (or too scary) to be true, it probably is a scam. For example, an online ad that says, "Get a grant of $5,000 now – limited time!" should raise suspicions. Train yourself to recognize these tactics and not react impulsively.

Protect Personal and Organizational Information: Be mindful of the information you share publicly on websites and social media, as it can be used against you in cyberattacks. Attackers often gather details from social media profiles or websites to craft more convincing phishing emails (a practice called spear phishing when highly targeted). For instance, if your CSO's site lists staff emails and interests, someone might email you referencing that information to earn your trust. Therefore, limit what you divulge about internal matters on public forums. When filling out web forms, consider whether all requested data is necessary. If a site asks for your mother's maiden name or other personal data without a clear need, think twice. From a privacy perspective, use privacy settings on social media to restrict who can see your posts. And for the organization, ensure that directories or sensitive documents aren't inadvertently exposed on your own website. Periodically search for your CSO's name online to see what info is out there – you might catch an exposed document or an impersonating site this way.

Use Updated Browsers and Security Tools: Safe internet use is not just about behavior; it's also about using updated technology. Always run the latest version of your web browser (Chrome, Firefox, Edge, etc.), since updates often patch security vulnerabilities. Enable the browser's built-in security features: most browsers have phishing and malware protection that can block known bad websites. You should also have a reputable antivirus/anti-malware program active on your device, which can sometimes detect if a download or site is malicious. Modern antivirus solutions often include web protections that warn or block if you attempt to visit a site known for phishing or hosting malware. For example, Microsoft Defender or Avast might flash a warning page if you try to access a dangerous site. Pay attention to these warnings; they are there to protect you.

To sum up, using the internet safely is largely about staying alert and skeptical when online. Much like street smarts in a big city – you remain aware of your surroundings and think twice before entering a dubious alley

– online, you should watch where you "travel" and with whom you interact. Encourage everyone in your team to adopt a cautious mindset: hover over links before clicking, only download from trusted sources, and treat unsolicited pop-ups or messages with suspicion. In the next section, we'll delve deeper into one of the most common avenues of attack, email and messaging, and how to secure those communications.

Email and Messaging Security

Email is an indispensable tool for CSOs, and messaging apps (like WhatsApp, Signal, or Telegram) are widely used for quick communication. However, these channels are frequent targets of cyberattacks such as phishing, eavesdropping, and account hijacking. This section provides guidance on how to communicate more securely and avoid common pitfalls.

Phishing Awareness: Email phishing was touched on earlier because it's so prevalent. To reiterate and expand: Always scrutinize unexpected emails, especially those urging immediate action or asking for sensitive info. A typical phishing email might appear to come from a colleague, a bank, or an online service, and contain a link to "log in" or an attachment to open. Before clicking any link in an email, verify the sender and the link target. Check the sender's address carefully – attackers often use an address that's off by a letter (e.g., john.doe@micros0ft.com instead of a legitimate Microsoft email) or a public email not matching the claimed organization. If an email claims you need to reset a password or provide information, it's safer not to click the email's link. Instead, go to the official website yourself. For attachments, do not open files from unknown or untrusted emails. Even if it's from a known contact, if it's unexpected and strange (e.g., a random document titled "Invoice" that you weren't expecting), verify with the sender through another channel. As a rule, avoid enabling macros or enabling content in Office documents unless you are absolutely sure of their source – many malware infections come via Word/Excel macros in phishing attachments.

CSOs should educate their staff that it's okay (even encouraged) to be a bit paranoid with emails – when in doubt, verify. A quick phone call or message

to the supposed sender could confirm if they really sent that request. It's better to double-check than to click and regret. Remember, phishing isn't limited to email; it can also occur via SMS (text messages with bad links) or messaging apps. For example, a staff member might get a WhatsApp message that looks like an alert from an online payment service with a link – treat those the same way, with caution.

Email Account Security: Because email accounts can be a gateway to reset other passwords and contain sensitive correspondence, securing your email login is crucial. Use a strong password and 2FA for your email account (as discussed in 2.1) – many email providers like Gmail, Outlook, or ProtonMail support two-factor authentication via an app or SMS. This drastically reduces the risk of someone hacking into your email. Also, be mindful when accessing email on shared or public computers; always log out afterwards and ensure the browser does not save your credentials. If possible, use secure email protocols (most modern services default to this): ensure the webmail uses HTTPS, and if you use an email client app (like Outlook, Thunderbird, or on your phone), make sure it's set to use encrypted connections (SSL/TLS) for both receiving (IMAP/POP) and sending (SMTP). Your IT support or provider's documentation can confirm these settings.

Consider email encryption for highly sensitive communications. Standard emails are not end-to-end encrypted, meaning in theory, email content could be read by unintended parties (like email providers or anyone who gains access to the account). For sensitive data, you might use tools like PGP/GPG email encryption or switch to secure messaging platforms for that conversation. However, PGP can be complex for everyday use, so another strategy is to use secure file-sharing for sensitive attachments rather than putting confidential text in the email body. Some CSO-focused email services or enterprise suites offer built-in encryption or at least the ability to password-protect emails or attachments. If your organization deals with extremely sensitive information (human rights cases, for example), you

should consult a digital security expert on setting up an encryption workflow.

Secure Messaging Apps: Many CSOs use instant messaging for quick chats and coordination. It's important to choose messaging apps that offer end-to-end encryption (E2EE), which ensures that only the communicating users (and no one in between, not even the service provider) can read the messages. WhatsApp, for instance, has E2EE by default for chats, as do Signal and Telegram's "secret chats" (note: Telegram cloud chats are not E2EE by default). Signal is widely recommended in the civil society community for sensitive communications because it is open-source, E2EE, and has strong privacy practices. Another is **Wire**, which is also secure and European GDPR-compliant. **Threema** and **Element (Matrix)** are other secure messaging options that some human rights groups use. The specific app choice may depend on your context and what your counterparts use, but a general rule is: avoid plaintext channels (SMS texts or unencrypted emails) for sensitive matters and migrate to an encrypted app where feasible.

Even with encrypted apps, be mindful of metadata (who is talking to whom, when). Most E2EE apps still reveal some metadata to the service (though Signal tries to minimize this). For extremely sensitive operations, one might use more anonymity-focused tools like *Session* or use messaging over Tor, but those are advanced scenarios. For general CSO use, a mainstream E2EE app will vastly improve security compared to unencrypted channels.

Also, lock down your messaging apps: Use app-lock features or device PINs so that if your phone is lost or stolen, someone can't just open your chats. Enable disappearing messages for highly sensitive conversations – many apps let you set messages to auto-delete after a certain time (Signal, WhatsApp, etc.). That way, if someone compromises your account later, past messages may already be gone.

Beware of Messaging Scams: Phishing scams do not abuse email only. You might get fraudulent messages via SMS or apps asking you to click a link (often shortened URLs) or to forward something. An example is the

"WhatsApp code" scam: you get an SMS with a login code you didn't request, then immediately a WhatsApp message from a friend saying, "I'm having trouble, please send me the code you just got." That friend's account is likely hacked, and the attacker is trying to use your code to take over your WhatsApp. The lesson: never give verification codes to others, and be suspicious of urgent, odd requests on chat, even if from friends.

Attachments and Cloud Links: Instead of attaching documents in email, many have moved to cloud links (e.g., Google Drive, Dropbox, OneDrive links). These are convenient but have their own security considerations. If you send a cloud sharing link, ensure it's only accessible to the intended people (use private links or add their emails explicitly) and consider setting expiration dates for the link. If you receive a cloud link, be cautious as with any link – make sure it's from a legitimate cloud service domain and that you expected it. A phishing tactic might send a link that looks like a Google Drive file but leads to a fake login page. Always confirm if needed, and ideally, access shared drives via the known interface (e.g., log into your Google Drive directly to see if a file was shared with you).

Email Hygiene and Best Practices: A few more quick tips: Use spam filters – modern email services do a decent job catching most junk/phishing. Still, check your spam folder occasionally for false positives, but don't interact with emails in spam unless you're sure they're safe. Don't unsubscribe from spam emails unless they are from reputable sources; clicking "unsubscribe" on truly spammy emails can confirm to spammers that your address is active. It's better to just delete them. When sending emails to large groups, use BCC to protect recipients' addresses from being seen by all (preventing accidental leaks of contact lists). And consider enabling email forwarding alerts or login alerts if your provider offers them, so you know if any unusual activity happens (for example, Gmail can notify you if a new login occurs from a new device).

By following these practices, your organization can significantly reduce the risk of falling victim to email or messaging-based attacks. Since email is often the first point of contact for attackers, mastering email security yields a

big security payoff. Think of it like safe driving: most of the time, the "roads" (internet) are fine, but you must wear your seatbelt (2FA), obey signals (warnings about suspicious links), and stay attentive to avoid accidents.

Basic Tips for Securing Computers and Phones

Laptops, desktop PCs, and smartphones are the workhorses of any modern organization. They also store a lot of sensitive data and can be entry points for attackers if not secured. This section provides fundamental tips to keep these devices safe from common threats. Many of these tips fall under routine maintenance and sensible use – the digital equivalent of locking your doors and getting regular oil changes.

Keep Software Updated: Ensure that all your devices' operating systems and applications are kept up-to-date with the latest security patches. Software updates often fix vulnerabilities that attackers might exploit. Turn on automatic updates wherever possible – for example, enable Windows Update or macOS' automatic updates, and do the same on your iPhone/Android phone for system and apps. Also, update your apps (browsers, office programs, etc.) regularly; many will prompt when an update is available – don't ignore those prompts. For any software that doesn't auto-update, set a recurring reminder to check for updates or use a centralized management tool if available. Remember that this includes browser plug-ins and frameworks like Java or Adobe Reader, which historically have been avenues for malware if outdated. An updated device is a hardened device.

Install Antivirus/Anti-Malware Protection: Use a reputable antivirus solution on your computers (and consider one of the reputable mobile security apps for Android devices as well). Modern antivirus software provides real-time protection, meaning it will actively scan files and monitor system behavior to block malware. Windows 10/11 comes with built-in Microsoft Defender, which is quite good for basic use if kept updated. Third-party options (paid or free) like Avast, Bitdefender, and ESET, etc., can also be considered. The key is to have something and keep its virus definitions updated daily. Avoid using multiple antivirus programs at once (they can

conflict). On phones, iPhones generally don't need separate AV apps due to how iOS is designed, but Android phones might benefit from an anti-malware app, especially if you sometimes install apps from outside the official Play Store. However, the best defense for phones is to only install apps from trusted app stores and check app permissions – a flashlight app, for example, shouldn't need to see your contacts or messages.

One more thing: never disable your security software out of convenience. If it blocks an action, investigate why rather than simply turning it off. Also, do not install pirated software, as mentioned – aside from legality, cracked software often comes bundled with trojans that antivirus software may or may not catch.

Use Device Locks and Encryption: Always lock your devices with a PIN, password, or biometric lock (fingerprint, facial recognition) when not in use. Set a short auto-lock timeout (e.g., screen locks after five minutes of inactivity or less). This prevents unauthorized access if someone physically gets hold of your device. If a CSO laptop is stolen from a car or a phone is lost at a conference, a strong lock screen can protect the data from prying eyes – but only if it's in place. For laptops, consider full-disk encryption. Modern operating systems often have this by default: Windows has BitLocker (Pro editions) or Device Encryption, and macOS has FileVault. When enabled, even if the hard drive is removed, data remains scrambled without the decryption key (usually tied to your login password). On smartphones, both iOS and Android support device encryption (newer versions encrypt by default when you use a PIN/password). Check that encryption is enabled, especially on older Android versions where it might have been optional. Encryption is crucial for sensitive data; for instance, if a laptop containing participant data for a study is lost but encrypted, the data remains secure, and the incident is a lost device problem, not a data breach.

Regular Backups: While backups are primarily a data recovery measure, they are also a security measure – they allow you to recover from ransomware or device loss without yielding to extortion or suffering total loss. Chapter 3 will detail backup strategies, but as a basic tip: back up

important files regularly and keep backups in a secure location separate from your computer (external drive stored safely, or a cloud backup service). Test those backups occasionally to ensure you can restore data. For mobile devices, consider backing up important photos/docs (phones can be set to back up to cloud or a computer). In case of phone theft, at least your data isn't gone forever.

Safe Installation of Apps/Programs: Only install software from trustworthy sources. On computers, that usually means the official website of the software or a known app store (like Microsoft Store or Mac App Store). On phones, use Google Play Store, Apple App Store, or F-Droid (for open-source Android apps). Be wary of free utilities from unknown websites – if you need a PDF converter or video player, for example, research a reputable one rather than downloading the first thing you find. Some malicious programs masquerade as useful tools. Also, during installation, pay attention to prompts and decline any offers to install extra toolbars or change your search engine (common in freeware installers). These aren't exactly security threats, but they clutter your system and can introduce vulnerabilities or privacy issues.

Secure Configuration and Settings: Take a moment to configure basic security settings on your devices. For example, on Windows, ensure the firewall is turned on (it usually is by default). A firewall helps block unwanted inbound connections. Most users won't need to adjust it beyond the default, but it should stay enabled. On your router, make sure firewall/NAT is on and remote admin is off (as mentioned in safe internet). On smartphones, check privacy settings for each app – disable unnecessary permissions (does a game need access to your microphone? Likely not). Both Android and iOS allow you to view what permissions each app has and revoke those that seem excessive.

Physical Security of Devices: Digital security isn't only digital – physically securing devices is important too. Don't leave laptops or phones unattended in public places. In the office, have a policy to lock screens when stepping away from your desk (Windows and Mac both have shortcuts for this). If

you are traveling, be mindful of laptops at airport security or in taxis – many breaches are simply lost devices with sensitive info. Also, consider privacy screens for laptops if you often work in public (to prevent shoulder surfing of your screen). For desktop computers, especially if your CSO has an office accessible to visitors or shared spaces, locking server rooms or using cable locks for equipment can deter theft.

Use of Mobile Device Management (MDM) for Organizations: If your CSO has the capacity (or as it grows), you might implement an MDM solution. MDM software allows an organization to enforce security policies on phones and laptops centrally – for example, requiring a PIN, pushing automatic updates, or remotely wiping a device if it's lost. Even without formal MDM, at least ensure you can remotely wipe devices: for phones, services like Find My iPhone or Android's Find My Device can remotely locate and erase a lost phone. For laptops, if using Windows linked to a Microsoft account or enterprise tools, there are sometimes similar options. At minimum, know how to change passwords and invalidate sessions for accounts on a lost device (for instance, if your volunteer loses a phone that had access to the CSO's email, immediately change that email password and sign out all sessions).

Plan for Failures: Sometimes, hardware fails or gets corrupted. While not a "cyber-attack," these events can cause data loss or downtime. Basic tip: use a reliable antivirus, but also keep some recovery tools handy (like a bootable clean USB stick with antivirus or system repair tools). And ensure important files aren't stored solely on one laptop; if hardware fails, you have backups or sync in place.

By applying these foundational tips, you create a baseline level of protection for your personal and work devices. Think of it as securing the "endpoints" – each phone or PC is an endpoint that can be exploited if weak, but collectively they form your CSO's digital environment. An attacker will often go for the easiest target. These measures (updates, antivirus, strong configurations) remove the low-hanging fruit, forcing adversaries to work much harder or ideally deter them entirely. It's analogous to home safety:

you lock doors, install smoke alarms, and maybe have a dog – none of this guarantees safety, but they greatly reduce risks and provide alerts. In cybersecurity, your updated, well-configured device with security software is like a home with locks and alarms – far less attractive to intruders than an unpatched, unprotected system.

With personal and device security habits in place, we now move to the organizational level: developing a plan and culture in your CSO that supports digital security. The next chapter will address how to assess risks and create a simple but effective **Digital Security Plan** tailored to your CSO's needs.

Chapter Summary

Chapter 2 provides an accessible introduction to fundamental cybersecurity concepts tailored for CSOs, focusing on the CIA triad: confidentiality, integrity, and availability. Confidentiality ensures data (e.g., donor records) remains private, integrity prevents unauthorized changes, and availability keeps systems accessible. The chapter uses plain language and CSO-relevant examples, like securing activist contact lists, to explain these principles. It introduces threat modeling, a process to identify risks and prioritize protections, making it relevant for resource-constrained organizations. Practical best practices include strong passwords, two-factor authentication (2FA), and cautious internet use. The chapter emphasizes low-cost solutions, such as free password managers (e.g., Bitwarden), to address CSOs' budget limitations. It also highlights the human element, noting that 74% of breaches involve errors like falling for phishing scams. By fostering awareness, CSOs can mitigate risks without technical expertise. The chapter encourages starting with simple steps (e.g., updating software) to build a security foundation. It connects digital security to CSOs' missions, explaining how protecting data upholds trust and accountability. For example, a compromised donor database could erode public confidence, as seen in past incidents. The chapter sets a practical tone for the e-book, equipping readers with foundational knowledge to implement security measures effectively.

Step-by-Step Guide for Conducting a Basic Risk Assessment

This guide provides a structured process for CSOs to complete the risk assessment template, with examples tailored to common CSO assets like donor databases and volunteer records. The steps are designed to be accessible for organizations with limited technical expertise, aligning with the curriculum's emphasis on practical frameworks (Module 2) and the e-book's guidance on risk assessment (Chapter 5).

Step 1: Identify Critical Digital Assets

- What to do: List the digital assets (data, systems, accounts) essential to your CSO's operations. Focus on what would disrupt your mission or harm stakeholders if compromised.
- How to do it: Gather a small team (e.g., leadership, program staff, IT focal point) to brainstorm. Consider data (e.g., donor lists, beneficiary info), systems (e.g., email, website), and accounts (e.g., social media, cloud storage).

Example:

» Donor Database: A spreadsheet or CRM system containing donor names, contact details, and donation amounts.

» Volunteer Records: Files with volunteer names, contact info, and schedules stored on a shared drive or cloud platform.

» Email Accounts: Staff Gmail or Outlook accounts used for communication with stakeholders.

Step 2: Identify Threats to Each Asset

- What to do: For each asset, list potential threats (e.g., hacking, phishing, malware, human error) that could compromise it.
- How to do it: Discuss how attackers might target the asset or what could go wrong (e.g., accidental leaks, device theft). Refer to common threats from the e-book (Chapter 1.3), such as phishing, data breaches, or ransomware.

Example:

» Donor Database:

– Threat: Data breach via phishing (attacker tricks staff into revealing login credentials).
– Threat: Ransomware encrypting the database.
» Volunteer Records:
– Threat: Unauthorized access due to weak passwords or shared credentials.
– Threat: Loss of data if a laptop is stolen.

Step 3: Assess the Likelihood of Each Threat

- What to do: Rate how likely each threat is to occur on a scale of 1 (Rare) to 5 (Almost Certain).
- How to do it: Consider factors like your CSO's visibility, past incidents, or common attack trends (e.g., phishing is widespread). Use local context if available (e.g., frequent phishing in your region).

Example:

» Donor Database:
– Phishing: Likelihood = 3 (Possible, as phishing is common, but your staff have some training).
– Ransomware: Likelihood = 2 (Unlikely, if antivirus is in place, but not impossible).
» Volunteer Records:
– Unauthorized Access: Likelihood = 4 (Likely, if passwords are weak or access isn't restricted).
– Laptop Theft: Likelihood = 2 (Unlikely, but possible in field operations).

Step 4: Assess Impact of Each Threat

- What to do: Rate the severity of the threat's consequences on a scale of 1 (Low) to 5 (Severe), considering mission disruption, data loss, or reputational harm.
- How to do it: Think about the worst-case scenario (e.g., legal issues, loss of trust, harm to beneficiaries). Reference the e-book's examples, like the Australian Red Cross breach (Chapter 1.1).

Example:

» Donor Database:

– Phishing/Breach: Impact = 5 (Severe, due to donor data exposure, GDPR fines, loss of trust).

– Ransomware: Impact = 4 (High, as operations could halt without backups).

» Volunteer Records:

– Unauthorized Access: Impact = 4 (High, as volunteer privacy violations could harm reputation).

– Laptop Theft: Impact = 3 (Moderate, if data is encrypted but recovery is costly).

Step 5: Calculate Risk Scores and Prioritize

- What to do: Multiply Likelihood by Impact to get a Risk Score (1-25). Higher scores indicate risks needing urgent attention.
- How to do it: Use the template to calculate scores and sort risks from highest to lowest. Focus on addressing high-scoring risks first.

Example:

» Donor Database:

– Phishing: 3 x 5 = 15 (High priority).

– Ransomware: 2 x 4 = 8 (Moderate priority).

» Volunteer Records:

– Unauthorized Access: 4 x 4 = 16 (High priority).

– Laptop Theft: 2 x 3 = 6 (Low priority).

Step 6: Develop Mitigation Steps

- What to do: List specific, actionable steps to prevent or reduce each threat, focusing on low-cost, practical measures.
- How to do it: Draw from the curriculum (Module 1-5) and e-book (Chapters 2-4) for solutions like 2FA, encryption, or training. Ensure steps are feasible for your CSO's resources.

Example:

» Donor Database:

– Phishing: Enable 2FA on database access, encrypt files, and train staff on phishing detection.

– Ransomware: Schedule weekly backups to a secure cloud, install updated antivirus software.

» Volunteer Records:

– Unauthorized Access: Use strong passwords, restrict access to authorized staff, and audit permissions monthly.

– Laptop Theft: Enable device encryption, use remote wipe tools for lost devices.

Step 7: Review and Update

- What to do: Assign a team member to review the risk assessment annually or after major changes (e.g., new software, staff changes). Update the template as needed.
- How to do it: Schedule a review meeting to check if assets, threats, or mitigation steps have changed. Document updates to ensure the plan remains relevant.

Example: After implementing 2FA, the likelihood of unauthorized access to volunteer records drops to 2, reducing the risk score to 8. Update the template accordingly.

2.3 CHAPTER

3: DIGITAL SECURITY PLANS FOR CSOS

A Digital Security Plan for CSOs

Having covered individual practices, we turn to the broader organizational approach. A digital security plan is a strategic and operational roadmap for how your CSO will protect its digital assets and respond to threats. It doesn't have to be a complicated or lengthy document. In fact, a concise plan that everyone understands is often better than a bulky policy that sits on a shelf. This chapter guides you through creating a basic security plan, focusing on **four key elements:** – Recognizing your risks,

- Formulating the plan with appropriate measures,
- Building awareness through training,
- Protecting your data through backups and secure storage.

Recognizing the Risks: What Threats Does Your Organization Face?

Every organization has a unique profile of risks depending on its activities, data, and adversaries. The first step in developing a security plan is to **identify and assess these risks** – essentially, to perform a simple digital risk assessment. This doesn't require an advanced degree; it means systematically thinking about what could go wrong and how badly it could hurt your operations if it did.

Identify Your Assets and Data: Start by listing the important digital assets and information your CSO holds. These include: hardware (computers, phones, servers), software and services (email accounts, websites, cloud drives, databases), and data (member lists, financial records, research data, communications, etc.). Ask questions like: What data would cause the most damage if made public? What systems are critical to our day-to-day work?

For example, a CSO that provides legal aid might prioritize client case files and communications with lawyers as critical assets to protect (due to confidentiality). A development CSO might identify its donor database and field research data as vital. Knowing what your "crown jewels" are will help focus your security efforts.

Identify Potential Threats and Threat Actors: Next, consider who or what might want to harm your organization's digital infrastructure. Some common threats are indiscriminate – e.g., random cybercriminals spreading ransomware for profit, which could hit anyone. Others might be more targeted: perhaps companies or individuals that oppose your advocacy, or even government surveillance if you work on sensitive issues. List out categories of threats: hackers looking for financial gain, insiders (staff or volunteers) who might accidentally or intentionally compromise security, and threats specific to your context (for instance, a CSO campaigning against corruption might attract targeted phishing or phone hacking attempts from affected parties). Also consider physical threats to digital assets, such as theft of equipment or destruction due to disasters (flood, fire – these can cause IT outages too, which is why backups off-site are needed).

For each threat, think about the possible scenarios: *How* could this threat manifest? For example:

- A cybercriminal might attempt to hack your website to deface it or use it to distribute malware.
- A hostile actor might send phishing emails to your staff, trying to steal passwords and read your emails.
- Malware like ransomware could infect a staff computer, encrypting files and demanding a ransom, as discussed in previous chapters.
- A volunteer could lose a laptop with unencrypted sensitive data.
- A disgruntled former employee might still have access to an account if offboarding wasn't done properly, posing a risk of data theft or sabotage.

Assess Likelihood and Impact: Not all risks are equal. While some events might be very unlikely but disastrous if they occurred, others might be likely but minor in impact. For each identified risk scenario, rate how likely it is to

happen (low, medium, high) and what the impact would be if it does (low, medium, high impact). For instance, *phishing attacks* are very likely (high likelihood) and could have a high impact (if account credentials are stolen) – so that's a high risk that needs strong mitigation. On the other hand, *hardware failure* is fairly likely over time (eventually a disk fails), but if you have backups, the impact is low, so it's a moderate risk that you manage with backups. Or *targeted state-sponsored hacking* might have a high impact (they could compromise deeply), but if you're a small local CSO with no high-profile campaigns, the likelihood might be low – still worth some protection, but not your No. 1 focus.

This kind of qualitative assessment helps you prioritize. As one CSO-focused guide suggests, understanding cyber risks and knowing what needs protecting are the first steps to effective security. You might even frame them as questions like Liberties' guide does: "What are our most important digital assets? Who might try to attack them and why? What would happen if X asset were breached or unavailable?" Bring your team into this brainstorming – different staff might highlight different concerns (e.g., finance officer worries about bank account credentials, communications officer worries about social media being hacked, etc.).

Consider Legal and Compliance Risks: CSOs also must think about regulations like data protection laws. In the EU, for example, GDPR requires organizations to protect personal data and report breaches. So, one risk of poor security is legal non-compliance and fines. If your CSO handles donors' or beneficiaries' personal information, a breach could mean violating privacy laws. Thus, include compliance in risk thinking – e.g., "Risk of personal data leak – impact includes harm to individuals + legal penalties." That risk would clearly be high impact, and if you have lots of personal data, perhaps medium likelihood, warranting strong controls.

***Document and Rank Risks*:** Write down a short risk register – even a simple table of risk scenarios, likelihood, impact, and current measures in place. Rank them by risk level (some combination of likelihood and impact). This will guide where to allocate resources. For example, you might rank

"Phishing attack leading to account compromise" as a top risk, while "DDoS attack on website" might be lower if your site isn't controversial and has cloud protections. Or "Insider accidentally leaking data via Google Drive link" might be a medium risk to handle via training and access controls.

Risk Appetite: It's also good to recognize that *no organization can eliminate all risk*. Part of risk management is deciding what level of risk is acceptable given your resources. This is often called your "risk appetite." A small CSO might accept the risk of not having a 24/7 IT security team and instead focus on basic defenses and external support when needed. The aim is to reduce risks to a level you're comfortable with. For high risks, you implement strong mitigations; for lower ones, perhaps more basic or monitor them over time.

By the end of this risk recognition phase, you should have a clearer picture of where you stand. For example, you may conclude: *Our biggest vulnerabilities are phishing and weak passwords (high risk), plus outdated software on our website (medium risk), and low awareness among volunteers (contributing to risks). We have a moderate risk from lost devices (we sometimes share laptops), but if we enable encryption, that can go down. We likely aren't specifically targeted by nation-states, but we handle sensitive community information that must be kept confidential.* These insights set the stage for crafting your security plan – essentially, the plan will address these identified risks with appropriate measures.

By knowing your organization's digital weak points and the threats most likely to exploit them, you can plan defenses efficiently. This approach aligns with the concept of risk-based decision-making – a core principle recommended in cybersecurity frameworks. It ensures you focus on what matters most, rather than trying to do everything everywhere. Now, with this risk picture in mind, let's proceed to building a plan that covers policies and practices to mitigate these risks.

Building a Simple Digital Security Plan

With your risks identified, the next step is to formulate a plan to manage and mitigate those risks. A digital security plan for a CSO typically includes

policies, procedures, and controls that address the main areas of risk, as well as outlines of roles and responsibilities. Don't be intimidated by the term "plan" – it can be as straightforward as a checklist or a short document. The key is that it should be practical and tailored to your organization's size and needs.

Security Policy and Governance: Start by establishing some guiding policies. This can be a brief section stating the organization's commitment to digital security and basic rules everyone should follow. For example, have a Password Policy (e.g., require strong passwords of a certain length and 2FA on all critical accounts – you can refer to Section 2.1 for specifics), an acceptable use policy (e.g., guidelines on using work devices and internet for appropriate purposes, not installing unauthorized software, etc.), and a Data Protection Policy (e.g., rules on handling personal data, following legal requirements like GDPR, and classifying data sensitivity). ENISA advises that clear cybersecurity policies should be written and communicated to employees, outlining how they are expected to behave with ICT resources and what consequences exist for non-compliance. For instance, your policy might state that staff must not share account passwords and must report any suspected phishing attempt to the IT focal point immediately.

If your CSO is small, you might roll many things into one general policy document – that's fine. The important part is assigning responsibility. Decide who in your team is in charge of security oversight (it could be an executive director or a tech-savvy staffer who becomes the "security point person"). ENISA's SME guide notes that assigning management responsibility for cybersecurity is a key element of success. So, explicitly name a role: e.g., "The Operations Manager will serve as the Information Security Officer, responsible for coordinating security efforts and ensuring policies are implemented." If you have a board or leadership, make sure they endorse this plan – leadership support is crucial for getting buy-in from everyone.

Risk Management Actions: For each major risk identified (from 3.1), outline what you will do about it. This effectively becomes the core of your

plan:

- For example, if "phishing" is a top risk, your plan might include actions like implementing 2FA on email (already discussed), conducting phishing awareness training (see 3.3), and setting up procedures to verify unusual requests (like a financial transaction confirmation process).
- If "outdated software" was a risk, your plan would include maintaining an inventory of key software and a schedule or responsibility for updates (perhaps the security point person or external IT support ensures updates monthly).
- If "data breach of personal info" risk was identified: plan measures like restricting access to that data (only certain people can access sensitive folders), using encryption for particularly sensitive files, and having an incident response procedure (in case a breach happens, how to contain and notify – more on that in Chapter 5).
- If "loss of device" risk: plan for full-disk encryption and remote wipe as mentioned, plus maybe a device check-in/out log for shared devices.

Incident Response Plan: A good plan, even a simple one, anticipates that things can go wrong. So, include a basic incident response procedure: if a cybersecurity incident occurs (like malware infection, suspected hack, etc.), who should staff report to, and what steps will you take? Chapter 5 covers this in depth, but in your plan, just outline roles: e.g., "All personnel must immediately report any suspected security incident to [Name/Role]. We will isolate affected computers from the network, assess the scope, and contact [IT support or external expert], if needed. We will also inform leadership and, if personal data is involved, prepare to notify affected parties and authorities as required by law." Having this in writing means that in the heat of a crisis, you have a reference to follow, which can save precious time and reduce panic.

Access Controls and Account Management: The plan should define how you manage user accounts and access. This might include maintaining a list of who has access to what systems, using the least privilege principle (give people access only to what they need), and, importantly, procedures for

onboarding and offboarding staff/volunteers. For example, when someone leaves the organization, your plan must ensure their accounts are promptly disabled or passwords changed. Many security incidents happen because former employees or partners still have active credentials. Include steps like "Upon staff departure, IT will revoke access to email, cloud drives, and any shared passwords within 24 hours." If you use shared accounts or generic logins (try to minimize those), have a plan to change those passwords routinely or when someone with knowledge leaves.

Third-Party Management: Recognize that your security also depends on any third-party services or contractors you use. If you identified "vendors" as a risk (e.g., an outsourced IT support or a cloud provider hosting your database), include measures to manage that. ENISA's guidance suggests ensuring all vendors with access to sensitive data meet security requirements and having contractual agreements on security. In a simple plan, this could mean verifying that any cloud service you use is reputable and compliant with data protection standards, and that you have backups independent of them if needed. Also, if you hire a web developer or IT consultant, ensure they sign an agreement to follow your security policies (like not reusing your credentials elsewhere or keeping data confidential).

Implement Baseline Controls: Summarize the concrete controls you will implement (some overlap with Chapter 2 tips, but here you formalize them):

- **Device Security**: "All organization laptops will have antivirus and firewall enabled, and full-disk encryption (BitLocker/FileVault) turned on. Automatic screen lock will be set to 10 minutes of inactivity."
- **Password Security**: "Enforce password policy: at least 12 characters, no common words, unique per account. Use of a password manager is encouraged and will be set up for staff. 2FA will be enabled on critical accounts (email, finance systems, etc.)."
- **Data Backup**: "Critical data (e.g., donor database, program files) will be backed up weekly to [secure cloud/encrypted external drive]. Test restores will be conducted quarterly."

- **Secure Configuration**: "Ensure default passwords on all equipment are changed. Disable unnecessary services on our website and keep it updated. Review user privileges periodically to remove excess admin rights."
- **Encryption for Data in Transit**: "Use encrypted channels for sensitive communications (e.g., Signal for confidential messaging, or PGP email for certain contacts as feasible). Our website has an SSL certificate (HTTPS), and we will enforce its use so that user submissions are encrypted."

While listing controls, avoid language that's too general or impossible to measure ("We will prevent all attacks" – unrealistic). Instead, focus on actionable controls. It might help to use a framework as a checklist – for instance, the CIS Controls (a popular list of basic cyber practices) or ISO 27001 domains for inspiration. But tailor it down to what you can implement.

Timeline and Maintenance: State how often the plan itself will be reviewed and who will maintain it. Tech and threats evolve, so maybe, "This security plan will be reviewed and updated annually (or whenever a major change in our IT occurs) by [Role]." Also, as you implement, you might not do everything at once. It's okay to prioritize actions in phases. Your plan could have a section "Action Plan" where you outline immediate steps (e.g., enable 2FA on email within 1 month, schedule training next month, implement backups by Q3, etc.). This turns it from just policy into a project with deadlines.

Communication and Enforcement: A plan only works if people know about it and it's enforced. Once drafted, share it with all staff and volunteers. Perhaps hold a short meeting to explain key points ("we now have a policy, here's what it means for your daily work"). Get feedback – maybe someone sees a gap or has a suggestion. Include in the plan or accompanying materials the consequences for non-compliance in a friendly way – e.g., "If policies are not followed, it may result in disciplinary action, but we aim to support everyone in achieving these best practices through training and

resources." This sets a tone that security is part of everyone's job, not just an IT thing. A good analogy from CyberPeace Institute: treat cybersecurity not as an isolated IT expense but as an **enabler** for your mission. By embedding security into everyday processes, you ensure continuity and trust in your operations.

To illustrate, imagine a small environmental CSO's security plan excerpt:

- **Risk**: Phishing of staff email – **Mitigation**: mandatory 2FA for email, training on phishing recognition (led by IT volunteer), and create a reporting protocol for suspicious emails.
- **Risk**: Loss of field laptops – **Mitigation**: full-disk encryption enabled, daily data sync to cloud when internet available, device lock codes in place.
- **Risk**: Website defacement – **Mitigation**: regular updates by web host, use of a security plugin or service, backups of site content, plan to quickly restore if hacked.
- **Policy**: All new volunteers must receive basic security orientation and sign the ICT usage agreement (covering not sharing accounts, etc.).
- **Responsibility**: Assigned Jane Doe (Program Manager) as security coordinator to monitor and guide these actions.

By mapping actions to risks and assigning who does what, your plan becomes actionable. It might only be a few pages long, but that's okay. Brevity can be powerful if it's clear. In fact, ENISA's SME guide distills advice into 12 high-level steps that serve as a mini-plan for businesses (things like "Develop good cybersecurity culture – assign responsibility," "Plan for incidents," and "Secure backups"). Many of those are mirrored here.

The final part of planning is implementing those measures and fostering awareness, which leads us to the next section. Keep your drafted plan handy as we discuss training and culture, since that's often one of the plan's components.

Awareness Training for Staff and Volunteers

Even the best security plan on paper can fail if the people in the organization aren't on board or knowledgeable. Human behavior is a critical

factor in digital security – as noted earlier, a significant majority of breaches involve a human element (errors or social engineering). Therefore, educating your team and building a culture of security awareness is one of the most impactful things you can do. Think of your staff and volunteers as the first line of defense (or conversely, the weakest link if not trained). This section outlines how to create and sustain effective security awareness training in a CSO context.

Start with the Basics: Training doesn't need to be overly technical. In fact, it's often better to focus on basic do's and don'ts, real examples, and interactive discussion. Cover the common threats in ways people can relate to. For instance, demonstrate what a phishing email looks like (perhaps show an actual phishing email that you sanitize for the training) and have people point out the red flags (poor grammar, weird sender address, unexpected attachment, etc.). Discuss a scenario: "If you get an email from the director asking for an urgent money transfer, what should you do?" (Answer: always verify by a phone call or face-to-face before acting, because it could be a CEO fraud scam). These practical exercises help staff realize how an attack might play out and how to respond calmly. ENISA recommends that training focus on **real-life situations** that SMEs face, which applies to CSOs as well. Adult learners often grasp concepts better through scenarios and stories than through abstract rules.

Key Topics to Include: At a minimum, address the topics from Chapter 2 in training form:

- Safe password practices and use of password managers.
- How to enable and use 2FA (perhaps a live demo of setting up an authenticator app).
- Recognizing phishing emails, suspicious links, and what to do (don't click, report it).
- Proper handling of sensitive information (e.g., using encrypted tools for confidential data, not using personal email for work content, etc.).
- Device security: importance of updates, not installing unauthorized apps, locking screens, and being careful with USB drives (unknown USB

sticks can be dangerous).

- Social media caution: not oversharing work-sensitive info on Facebook/Twitter, being mindful of social engineering (like someone calling pretending to be IT support).
- Reporting incidents: emphasize a no-blame culture. People should feel comfortable reporting if they clicked something bad or lost a device, rather than hiding it. Make it clear that prompt reporting is crucial, and they won't be punished for an honest mistake – the priority is to fix the issue.

Interactive and OCSO-ing Training: Awareness isn't a one-time event. Plan to have refresher sessions or at least periodic reminders. Many organizations do an annual security training. But in between, you can share tips in staff meetings or send a "security tip of the month" email. For example, in October (Cybersecurity Awareness Month, which is often promoted in the EU by ENISA), you might hold a fun quiz or share a short video on security. The training doesn't have to be dry. Some CSOs invite a security expert or use free online modules (there are many free cybersecurity awareness courses and videos targeted at nonprofits and small businesses).

Consider also leveraging external resources: If you have an IT partner or if there's a local tech university, sometimes they can assist in giving a workshop. There are also nonprofit initiatives that offer free cyber awareness workshops to civil society (for instance, organizations like TechSoup or CyberPeace Builders volunteers may help conduct trainings).

Special Focus for Key Roles: Tailor parts of the training to roles. Your finance officer might need deeper training on spotting invoice fraud or securing banking logins (because CSOs have been scammed via fake invoices or "CEO impersonation" emails into sending money to fraudsters). Your communications staff handling social media might need tips on avoiding account takeovers (like using 2FA and being wary of phishing DMs). Leadership should understand their role too – executives are often targets of spear phishing (the "boss" email trick), so they should model good

behavior (like never requesting sensitive info or transfers by just email without verification). Also, ensure volunteers or short-term staff get at least a mini onboarding in security, since they might not attend formal staff training. A one-page cheat sheet or quick briefing on "do's and don'ts" when they join can help.

Create a Culture of Questioning: Encourage everyone that it's okay to question things that seem off. For example, if a volunteer gets an unusual IT instruction that they're not sure about, they should ask. Make sure they know whom to ask – e.g., "If you receive any suspicious communication or are uncertain about a file or link, contact our IT focal point (or security coordinator) at [contact]." This goes back to the Microsoft advice: cybersecurity is a *team sport*, and if you see something, say something to a trusted advisor. If someone thinks they might have made a security mistake, such as clicking a bad link, they should feel safe to report it immediately rather than fear blame. Quick reaction can often avert or minimize harm (like disconnecting a PC if malware is suspected).

Measuring and Reinforcing: It helps to gauge how well your training works. One way is to conduct internal phishing tests (if resources allow): send a harmless "fake phishing" email to staff after training to see who clicks. Those who do can get a gentle follow-up training. But if you're a very small organization, informal Q&A and discussions might be enough to sense understanding. Even asking in a staff meeting, "What would you do if you get an email attachment from someone you don't know?" and hearing responses can reveal comprehension. Reinforce messages by posting a short list of security tips on the office bulletin board or Slack channel. Some organizations even incorporate security into staff performance reviews or routines ("Did you complete the annual security quiz?"), But in CSOs, a lighter approach often suffices unless you're handling extremely sensitive data.

Stay Informed and Share Updates: The threat landscape changes. If you become aware of a new relevant threat, update your team. For instance, if a fellow CSO reports a phishing campaign targeting organizations in your

sector, alert your staff: "Heads-up, there's a phishing email going around claiming to be from a funder – do not click any such emails, and notify us if you receive one." Being part of CSO networks or security info-sharing groups (as we'll see in Chapter 6) can provide such intel that you can pass on. This keeps security awareness current and shows staff that threats are real and happening in their environment, not just theoretical.

To summarize, awareness training turns your people from potential liabilities into assets in your security posture. As one cybersecurity slogan puts it, "Your employees are your best firewall." By fostering knowledge and a vigilant mindset, you greatly reduce the chance of a costly mistake. Remember, technology alone is not enough – even the strongest firewall can be bypassed if a user unknowingly lets the attacker in. But a well-trained team, supported by a positive security culture, can stop many incidents before they start, or catch them early. This human factor empowerment is at the heart of resilient digital security for civil society.

Protecting Your Data: Backup and Secure Storage

Data is often described as the "lifeblood" of organizations. For CSOs, data might include beneficiary information, research findings, donor details, financial records, project reports, photographs, and more. Protecting this data is not just about preventing unauthorized access (confidentiality), but also about ensuring it's not lost (availability) and not improperly altered (integrity). In this section, we focus on two fundamental aspects of data protection: regular backups and secure storage (both physical and in the cloud).

The Importance of Backups: Imagine the worst-case scenarios – a ransomware attack encrypts all your files, or a fire/flood destroys your office computers, or an intern accidentally deletes a crucial folder. In each of these cases, having a recent backup can literally save your organization. A backup is a separate copy of your data kept on a different medium (and preferably in a different location) that you can restore from if needed. Without backups, any of the scenarios above could mean irretrievable loss. With backups, you have a safety net.

Here are backup best practices, many of which align with standard advice:

Regular Frequency: Back up your important data regularly. "Regularly" depends on how often the data changes and how critical it is. For fairly static data, weekly might suffice; for rapidly changing data (like daily program logs or active databases), daily or even multiple times a day might be better. Determine your Recovery Point Objective (RPO): how much data could we afford to lose? If it's a day's worth, then daily backups are okay. If losing even one hour of data would be catastrophic, aim for more frequent snapshots.

Automate It: Human-dependent backup processes often fail due to forgetfulness or busy schedules. Use automated backup solutions when possible. For instance, set your file server or NAS to back up to an external drive every night at 2 a.m. Or use cloud backup services (like Backblaze, Acronis, etc.) that run continuously or on schedule. Many cloud storage services, like Google Drive or OneDrive, also keep previous versions of files, which can serve as a form of backup for file edits or deletions.

Multiple Copies & Off-site: Follow something like the 3-2-1 rule: 3 copies of data (primary + two backups), on 2 different media, 1 of which is off-site. This might be overkill for a very small CSO, but the idea is sound. You could, for example, have one backup on an external hard drive in the office and another encrypted backup in a cloud service. Off-site means that if the office burns down, the off-site (or cloud) backup is safe. Cloud backups inherently are off-site. If using physical media, consider storing a drive at a board member's house or a safety deposit box, updating it periodically.

Secure Your Backups: A backup is a copy of your sensitive data, so protect it. If you use an external drive, encrypt that drive (many backup tools or OS like Windows BitLocker can encrypt external disks). If using cloud backup, ensure the service encrypts data (most do, but you might also choose to encrypt files before uploading for extra security). Limit who can access backups. For example, don't leave a backup drive plugged in all the time to a system that's online – if ransomware hits, it could encrypt that too. Ideally, backups that are not constantly connected (offline backups) are immune to malware in your network. If using a network drive for backups, ensure it has

versioning or some safeguard that malware can't immediately corrupt old backups.

Test Restores: Backups mean little if they don't work when needed. At least a few times a year, test the restore process. Try to recover a file from backup and see if it opens correctly. Do a fire drill: "What if our main shared drive died – can we restore last night's backup onto a new device easily?" Testing will reveal any issues like corrupted backup, missing encryption keys, or procedures that need refining. Many organizations have discovered in crisis that their backups were incomplete or failed quietly long ago – don't let that happen to you.

Document Backup Procedures: Write down what is backed up, how, and where. Also note who is responsible for overseeing backups and how to perform a recovery. For instance: "Our Salesforce donor database is backed up by Salesforce's own daily export and additionally by a manual export by John on the 1st of each month to an encrypted USB drive." If John leaves, someone else can read that and continue the practice. Also, document credentials needed for backups (securely, of course), so you're not scrambling to find a password during an emergency restore.

Secure Storage and Access Control: Beyond backups, protecting data also means storing it securely in day-to-day use. This includes both physical storage (like printed files, USB drives, and servers) and cloud storage solutions:

Physical Files and Devices: If you have sensitive info in physical form (paper documents, USB sticks, external hard drives), store them in locked cabinets or a safe. Don't leave documents with personal data lying around on desks. For example, volunteer sign-up sheets or beneficiary forms should be filed away when not actively used. Shred sensitive documents before disposal. For devices, as discussed, use full-disk encryption so that if a computer or drive is lost, the data isn't easily accessed. Keep an inventory of devices – know who has which laptop or phone. If a device contains sensitive data, consider policies that it not be left in insecure places (e.g., locked in an office drawer or taken home by staff and kept securely). During

travel, perhaps use privacy screen filters and keep devices with you (don't check laptops in luggage if possible).

Cloud Storage (Google Drive, Dropbox, etc.): Cloud services are very convenient and have built-in redundancy, but you must configure them correctly for security. First, enable 2FA on the cloud accounts to prevent unauthorized logins. Second, manage sharing permissions carefully. Instead of sharing a whole drive openly, share folders/files only with specific people who need access. Periodically review who has access to what in your Google Drive or Dropbox – remove anyone who no longer needs it (including external collaborators whose projects ended). Be cautious with "share via link" features; if you create a public link to a file, theoretically, anyone who finds that link can access it (some systems now offer password-protected links or expiring links; use those if needed). For highly sensitive files, consider using client-side encryption before uploading (some tools integrate with Dropbox/Google Drive to encrypt files locally so that even if someone hacks your cloud account, they see gibberish without your key).

ENISA's guidance on cloud for SMEs echoes these points: understand the unique risks of cloud and ensure you choose reputable providers. They specifically note to ensure using providers that don't breach laws regarding data (like GDPR restrictions on storing personal data outside the EU without safeguards). For example, if your CSO operates in the EU and stores personal data, you should verify where your cloud provider stores data and possibly sign Data Processing Agreements. If you use services like Dropbox or Google, look into their compliance and maybe opt for those with servers in regions you trust or use a European alternative if needed.

Encryption in Transit and at Rest: Ensure data is encrypted not just on disks but also when transferring. Most cloud providers do encrypt data at rest on their servers and use HTTPS for transfers, which is good. If you self-host any data (like an on-site NAS accessible over the internet), set up a VPN or at least ensure Web connections are over HTTPS. Also, for extremely sensitive information, you might layer encryption – for instance, encrypt a document with a password before uploading to even an encrypted

cloud folder (double encryption). This might be relevant for, say, lists of activists in a hostile region.

Data Segmentation: Not everyone in the CSO should automatically have access to all data. Use access controls to segment data. For instance, HR files or staff medical info can be restricted only to HR personnel. Financial records are only to finance team. Project files only to those on that project, etc. Many cloud platforms allow permission tiers and group-based access. This way, if one user's account is compromised, the attacker doesn't necessarily get everything, only what that user could access. It also reduces internal misuse risk – people can't snoop on data unrelated to their role.

Plan for Data Retention and Destruction: Part of secure storage is not keeping data longer than necessary. Old hard drives from replaced computers should be securely wiped or destroyed (simply deleting files is not enough; use software to overwrite or physically destroy the disk). Same for USB sticks that are no longer used. If your CSO accumulates decades of personal data with no need, consider a policy to archive or delete old records. This reduces the amount of sensitive info that could be exposed in a breach and aligns with principles of data protection laws (minimize data retention). For example, if you ran a training five years ago and still have participants' ID copies, decide if you truly need those now.

Redundancy and Business Continuity: Backups ensure data continuity, but think about operational continuity too. If your office server crashes, having data backup is step one, but step two is restoring functionality. Your plan might include having a spare device or a cloud failover. For many small CSOs, working from cloud services for critical functions (email, docs, etc.) inherently provides continuity – you can continue work from anywhere on another device if one fails. But identify any single points of failure. If only one person knows how to access backups, that's a risk – cross-train someone else or document it, as mentioned.

Example Implementation: Suppose your CSO has a shared drive on a NAS device in the office for all project files. You implement a nightly backup of that NAS to an encrypted external HDD that your director takes home on

weekends (offsite). Additionally, critical subfolders are synced to a secure cloud (like Google Drive or Nextcloud) in real-time for collaboration and off-site safety. You schedule backups of your donor database from your CRM and download a copy monthly, which you encrypt and store in the cloud. For physical files like signed beneficiary consent forms, you scan and upload them (so they're backed up) and keep originals in a locked cabinet. For any laptops, you ensure BitLocker is on, and each has a BIOS/firmware password so thieves can't boot from USB to bypass encryption easily. Once a quarter, you simulate a data loss scenario to ensure you can restore from your backups.

By doing all this, you achieve resilience: even if a cyber disaster strikes or hardware fails, your data is safe, and you can resume work with minimal disruption. CyberPeace Institute has highlighted that nonprofits should view cybersecurity (and by extension, data protection measures) as enabling them to leverage tech safely for social impact. Secure data and backups mean you can embrace digital tools without constant fear of losing critical information.

In conclusion, backups and secure storage are like the seatbelt and airbags of your digital operation – you hope to never need them in an emergency, but if you do, they can save your organization from catastrophic losses. Combine that with the proactive measures from earlier sections (like password hygiene and access controls), and you create a strong shield for your CSO's information assets. Next, we will explore some of the easy-to-use tools that can further bolster your security in practice, complementing the plan and policies we've established.

Chapter Summary

This chapter offers practical guidance for CSOs to secure communications and sensitive data, critical for daily operations and trust. It covers encryption for email, messaging, and data storage, recommending tools like Signal for secure chats and HTTPS for web traffic. Strong access controls, such as robust passwords and 2FA, are emphasized to prevent unauthorized access to accounts like email or cloud platforms (e.g., Google Drive). The chapter advocates regular backups to secure locations (e.g., encrypted drives) to recover from ransomware or data loss, citing a case where backups saved a CSO from a ransomware attack. Secure file-sharing methods, like encrypted cloud services, are highlighted to protect beneficiary data. The chapter addresses GDPR compliance, stressing lawful data handling and consent. It includes actionable steps, such as enabling 2FA on Gmail or using free encryption tools, making it accessible for non-technical staff. Examples, like a charity's email hack via phishing, underscore the need for vigilance. The chapter also covers safe video conferencing and social media practices, ensuring CSOs can communicate securely in remote or high-risk settings. By implementing these measures, CSOs safeguard sensitive information, maintain operational continuity, and build donor trust.

Cybersecurity Plan Annual Review and Update Checklist for CSOs

This checklist ensures your CSO's cybersecurity plan remains current and effective by reviewing assets, threats, policies, and incident response strategies annually or after significant changes (e.g., new systems, staff turnover). Completing these steps maintains a robust digital security posture to protect your mission and stakeholders:

1. Review and Update Digital Assets

- Identify new or changed digital assets (e.g., new donor database, cloud storage, social media accounts) added since the last review.
- Remove obsolete assets (e.g., discontinued software, old email accounts) from the plan.
- Example: Added a new CRM system for donor management? Include it in the risk assessment. Retired an old volunteer database? Remove it from the plan.

2. Assess New or Evolving Threats

- Review recent cybersecurity trends or threats relevant to CSOs (e.g., increased phishing, ransomware, or local surveillance risks).
- Consult local resources (e.g., national CERT, CSO networks) or global reports (e.g., Microsoft's CSO attack statistics) for updates.
- Update the risk assessment template to reflect new threats or changes in likelihood/impact.
- Example: Noticed a rise in phishing emails targeting CSOs in your region? Increase the likelihood score for phishing in your risk assessment.

3. Review Recent Incidents or Near-Misses

- Document any cybersecurity incidents or near-misses (e.g., phishing attempts, malware alerts) since the last review.
- Analyze what went well and what failed in your response (e.g., did backups work? Was the incident reported promptly?).
- Update the plan with lessons learned to improve future responses.

• Example: A staff member clicked a phishing link, but 2FA prevented access. Add a note to reinforce 2FA training and update email filters.

4. Update Incident Response Procedures

• Verify that the incident response plan includes current steps, roles, and responsibilities (e.g., who detects, contains, communicates).

• Update contact lists for internal responders (e.g., IT staff, leadership) and external support (e.g., local CERT, legal counsel).

• Test the plan with a tabletop exercise (e.g., simulate a ransomware attack) to identify gaps.

• Example: New IT manager? Update their role as the incident response lead. Old CERT contact outdated? Replace with current details.

5. Check Security Policies and Compliance

• Review and update security policies (e.g., acceptable use, data protection, BYOD) to reflect new tools, regulations, or practices.

• Confirm compliance with data protection laws (e.g., GDPR, local regulations) and update procedures if needed (e.g., consent forms, breach reporting).

• Example: GDPR requires breach notification within 72 hours. Ensure your policy includes this timeline and a designated reporting contact.

6. Verify Technical Protections

• Audit security measures (e.g., 2FA, antivirus, backups, encryption) to ensure they are active and updated on all devices and accounts.

• Check for new security features in tools (e.g., cloud platforms, email providers) and enable them if applicable.

• Example: Google Workspace added a new security feature for shared drives? Enable it and update access controls.

7. Plan Staff Training and Awareness

• Schedule cybersecurity training or refreshers (e.g., phishing awareness, password management) for all staff and volunteers.

- Incorporate new topics based on recent threats or incidents (e.g., AI-driven phishing, cloud security).
- Example: After a local ransomware spike, add a 30-minute session on recognizing ransomware warning signs.

8. Test Backups and Recovery

- Verify that backups are running as scheduled and stored securely (e.g., encrypted cloud or external drive).
- Conduct a backup restore test to ensure data can be recovered quickly and accurately.
- Example: Restore a sample file from last month's backup to confirm it's accessible and intact.

9. Engage Leadership and Stakeholders

- Brief leadership on the updated plan and any resource needs (e.g., budget for new tools, time for training).
- Share key updates with stakeholders (e.g., donors, partners) to reinforce trust in your security practices.
- Example: Inform donors that you've strengthened data protection to comply with GDPR, enhancing transparency.

10. Document and Schedule Next Review

- Record all updates in the cybersecurity plan and store it in a secure, accessible location (e.g., encrypted shared drive).
- Schedule the next annual review or trigger a review after major changes (e.g., new software, office move).
- Example: Set a yearly calendar reminder to repeat this process.

2.4 CHAPTER

4: USER-FRIENDLY SECURITY TOOLS

User-friendly Security Tools

Thus far, we've covered practices and planning. In this chapter, we focus on the tools and technologies that can make implementing security easier. The good news is that you don't need to be a tech wizard or invest in very expensive solutions to get a solid level of protection. There are many **user-friendly, cost-effective tools** available – often designed with nonprofits or small businesses in mind – that can significantly enhance your digital security. We'll go through categories of tools: identifying secure applications, safe browsing aids, securing cloud storage, and tools for protecting your computers and phones. Each subsection introduces key tools or methods, with an emphasis on practicality and ease of use.

Recognizing Secure Applications

With countless software and apps available, how do you know which ones are "secure"? Here we outline some criteria and examples to help you choose applications that prioritize security and privacy.

What Makes an Application Secure? A secure app typically has the following attributes:

- It comes from a reputable developer or source and is actively maintained (updated regularly to fix bugs).
- It uses encryption to protect data in transit and at rest (especially important for communication and storage apps).
- It has good access control (e.g., allows strong authentication, maybe 2FA for accounts).
- It has a track record of responding to vulnerabilities (developers issue patches) and ideally has undergone security audits.

- The app respects privacy (doesn't collect excessive data or serve shady ads that could inject malware).

For instance, messaging apps like Signal are considered secure because they are open-source software (anyone can inspect the code for backdoors), use end-to-end encryption by default, and do not collect metadata unnecessarily. On the other hand, some free applications might seem handy but could be insecure – for example, a random file-sharing app that is not encrypted or a password manager with no 2FA option would be less secure than alternatives.

Choosing Software for Key Tasks: Here are some common categories of applications with secure recommendations:

***Password Management*:** Use a dedicated password manager app as mentioned. Good options include Bitwarden (open-source, cloud-based, free for basic use), LastPass (popular, has a free tier, though it had a breach in 2022, which underscores the need to use strong master passwords), 1Password (paid, user-friendly), or KeePass (open-source, offline). These have strong encryption to store your login credentials securely, and many support 2FA for unlocking the vault. They can also generate random passwords for you. Using any of these is far superior to keeping passwords in a spreadsheet or reusing them.

Secure Messaging and Email: For messaging, as discussed: Signal for most secure conversations; WhatsApp is also end-to-end encrypted (and widely used, although owned by Meta, it has strong encryption fundamentals). Wire or Threema can be good for organizational use if you want a European-hosted solution. For email, if you need higher security, consider providers like ProtonMail or Tutanota, which offer end-to-end encryption (especially for internal emails or emails between users of the same service). If sticking with Gmail or Outlook.com, they are reasonably secure if used with 2FA, but sensitive emails might be better sent via an encrypted channel or using tools like GnuPG/PGP for encryption (though PGP is complex in practice).

Antivirus/Anti-Malware: Use well-known, well-reviewed antivirus solutions as mentioned. Windows Defender (built-in on Windows 10/11) is a solid baseline and hassle-free. If you want a third-party: Avast, AVG, Bitdefender, Kaspersky (noting some have concerns with Kaspersky due to origin, but technically strong), ESET, etc. Many of these have free versions for basic protection. Pick one that doesn't overly slow down your system and has a good detection rate (independent AV test labs can guide this). Keep it updated.

Firewall and Network Security: For most, the built-in OS firewall is fine. If you need more control and visual cues (for advanced users), tools like ZoneAlarm or TinyWall on Windows can offer application-level firewall management in a friendlier interface. On your router, ensure its firewall is on. Some CSOs opt for hardware firewalls or UTM devices if they have an office network, but those can be complex; often, a good router (with updated firmware) acts as a basic firewall. If you operate a website, using a service like Cloudflare or your host's security add-ons can provide a firewall against web attacks.

Secure Browsers and Extensions: Use a modern secure browser (Chrome, Firefox, Edge, Brave). All are fairly secure; Brave is known for privacy defaults (blocking trackers). Firefox is open-source and highly configurable for privacy. Chrome is very robust in security (Google Project Zero finds exploits and patches aggressively), but sends data to Google (though mostly benign usage stats). Edge is also fine (built on Chrome's engine with Microsoft security features). You can enhance any browser with extensions: e.g., HTTPS Everywhere (now largely redundant since most sites auto-HTTPS, but it ensures encryption when possible), uBlock Origin, or Privacy Badger to block malicious ads and trackers (which also reduces risk of malvertising), and the browser's own pop-up blocker and anti-phishing filter should be on. Some use NoScript (blocks all scripts by default), but that's advanced and can break sites; it's optional for power users concerned about script-based attacks. Ensure click-to-play for Flash/Java (most browsers now disable Flash entirely, which is good).

VPN Services: If your team often uses public Wi-Fi or works remotely, using a VPN can add security. A *good* VPN service encrypts your internet traffic and can prevent local network snooping. It also hides your IP, which can add privacy. However, only use reputable paid/free ones (some free VPNs have been caught doing the opposite of privacy – logging or injecting ads). Alternatively, if you have the IT capability, you can set up your own VPN on a cloud server for your team. Simpler: many routers now support creating a home office VPN so staff can tunnel back to the office network securely when abroad.

Disk Encryption Tools: On top of OS built-in encryption, there are tools like VeraCrypt (free, open-source successor to TrueCrypt) that can create encrypted containers or encrypt entire drives. Useful if you want to encrypt USB sticks or create an encrypted folder (container file) that you can store anywhere (even the cloud) and know it's secure. VeraCrypt is a bit techy but well-documented. There are also simpler vault apps for phones and computers that password-protect and encrypt specific files (e.g., 7-Zip can create encrypted archives for files).

Safe Alternatives and Updates: As part of recognizing secure apps, sometimes it means replacing a risky app with a safer alternative. For example, if someone is using an outdated version of an app that's known to have vulnerabilities (say, an old CMS for a website or an old Adobe Acrobat), update it or switch to alternatives (like use Chrome's PDF viewer or SumatraPDF instead of an old Adobe Reader, which was a common target for malware). Replace end-of-life software (like Windows 7, which no longer gets updates – upgrade to Windows 10/11 or use a lightweight Linux if budgets are a constraint).

Mobile Apps: On phones, only install apps from official app stores, as emphasized. For secure communications, again Signal, WhatsApp (with caution about backups, as WhatsApp cloud backups can be unencrypted unless you opt-in to their new encrypted backup feature). For secure storage on phones, use built-in secure folder features (Samsung Secure Folder) or apps like **KeePassDX** for Android to manage passwords offline.

Training on Tools: Introducing new apps is only good if people use them correctly. So, part of rolling out any tool (like a password manager or VPN) is to give a short tutorial or cheat sheet. Many tools are intuitive, but initial guidance ensures proper usage (e.g., showing how to share passwords securely via the manager rather than by email).

By carefully selecting and using secure applications, you reduce vulnerabilities. However, keep balance: "most secure" sometimes means less user-friendly, which can lead to workarounds that introduce risk (like if a secure messaging app is too cumbersome, staff might revert to using open email for convenience). Choose tools that your team can comfortably adopt – often, mainstream tools configured well provide both security and usability. For example, Google Workspace or Microsoft 365, if set up with 2FA and proper admin controls, offer strong security for email/docs and are user-friendly. They might not be as locked-down as some niche solutions, but if people actually follow security practices on them, they can be sufficient and easier to integrate.

In essence, recognizing secure apps is about doing a bit of homework before installing something new and favoring those known for security. Many civil society organizations share lists of recommended tools (like Front Line Defenders' Security-in-a-Box, which offers tool guides). In the next sections, we'll highlight specific realms (web browsing, cloud, devices) with particular tips and tools for each.

Safer Browsing on the Internet

Web browsing is such a common activity that it's easy to forget potential dangers. This section builds on safe internet use practices from Chapter 2, now focusing on tools and browser settings that can make web surfing safer and more private.

Browser Security Settings: First, ensure you configure your web browser's built-in security features:

- Keep the browser updated (most auto-update by default; don't disable that).

- Enable phishing and malware protection (browsers like Chrome, Firefox, and Edge have this on by default, which checks visited URLs against known bad lists and shows a big red warning if a site is suspected of phishing or contains malware).
- Turn on "Do Not Track" (though largely advisory, some sites honor it).
- Consider using the browser's sandbox or site isolation features if available (Chrome has site isolation to mitigate certain attacks –usually on by default for high-risk domains).
- In Chrome, you can also use "Enhanced Safe Browsing" mode, which shares more data with Google for improved threat assessment (optional if you trust Google with that data).

Ad-blockers and Script Blockers: As noted, many malware infections occur via malvertising or malicious scripts on compromised sites. Using a reputable ad-blocker extension like **uBlock Origin** or **Adblock Plus** helps not only privacy and aesthetics but also security by cutting off common malware delivery vectors. These extensions block known ad domains and can prevent suspicious scripts from loading. Privacy-oriented ones like **Privacy Badger** (from EFF) learn to block trackers and often kill malicious third-party content in the process. If you're very concerned or visiting risky sites, **NoScript** (Firefox) or **ScriptSafe** (Chrome) can block all scripts by default – highly secure but requires manual whitelisting for legitimate site functionality, which can be burdensome unless you're tech-savvy. You might use a lighter approach: **Firefox** in strict Enhanced Tracking Protection mode, or the **Brave** browser, which by default blocks many scripts and ads.

Secure Connections and Extensions: Always try to use HTTPS versions of websites. The *HTTPS Everywhere* extension (from EFF) automatically redirects to HTTPS when possible, though these days most major sites default to HTTPS anyway. The browser padlock icon is your friend – click it to inspect certificate details or at least to ensure it's present for any site where you enter passwords or sensitive data. If you use public Wi-Fi often, consider an extension like **HTTPS Everywhere** (if not using a VPN) to ensure encryption, or just be vigilant manually. Some modern browsers

(Chrome, Firefox) now mark non-HTTPS pages that have forms as "Not secure" in the address bar – heed that warning.

Search Engines and Tracking: Google search is powerful, but it tracks queries. If you want to avoid targeted ads or profiling, consider **DuckDuckGo** as your default search engine. It doesn't track searches and has decent results for general queries. It also offers an extension that rates sites' privacy practices and enforces encryption. Alternatively, **Startpage** gives Google results but strips away identifying info. These can slightly improve privacy without much sacrifice in the quality of search.

Avoiding Poisoned Search Results: Sometimes malware sites or phishing pages appear in search results (e.g., fake tech support sites). Train staff to be cautious when clicking obscure search results and maybe stick to known websites for downloads (e.g., get software from an official source, not from a random aggregating site). Using an extension like **Web of Trust (WOT)** or **Bitdefender TrafficLight** can give reputation icons next to search results, indicating if a site is deemed safe by the community/algorithm – though such tools themselves have had controversies (WOT was found collecting user data, so use with caution).

Private Browsing Mode: Use "Incognito" or private mode in browsers when appropriate – it doesn't make you anonymous on the internet, but it doesn't save cookies, history, or cache after you close it. This is useful if you are logging into a service on a shared computer or if you just want to ensure no remnants remain of a particular session (like testing how your website appears to a new user). Note: It's not a security tool per se against external threats, but it can prevent other users of the same computer from snooping your sessions.

Tor Browser for Anonymous Browsing: For situations where you need a high-level anonymity or to bypass local internet censorship, the **Tor Browser** is a tool to consider. It routes your traffic through the Tor network, concealing your IP and encrypting traffic within the network (though traffic exits to the destination unencrypted unless using HTTPS). CSOs, journalists, and activists sometimes use Tor to reach blocked sites or avoid

surveillance. The downside is it's slower, and some sites block Tor exit nodes. But it could be part of your toolkit in repressive environments or for sensitive research. Only use the official Tor Browser from torproject.org and understand its usage guidelines (e.g., don't install extra browser plugins in Tor Browser, don't open documents while online as they may bypass Tor, etc.). If not needed for your context, a well-configured normal browser with a VPN might suffice.

Browser Choice Considerations: Using a diversity of browsers can sometimes sandbox activities. For example, you might use one browser exclusively for logging into sensitive accounts (and with minimal extensions, only security ones) and another for casual browsing. That way, the casual one can have all the experimental extensions or might occasionally visit less secure sites, while the "secure browser" (say, Firefox) you treat carefully (no unnecessary extensions, strict settings, only going to known sites like your bank, email, etc.). This limits the exposure of critical session cookies or data.

Email/Web Integration: Many modern email services will open links or attachments in some kind of sandbox or safe viewer (Google has its "Protected view" for attachments, Outlook Web has safe links if enabled by admins). If you have those features, keep them on; they add an extra layer, opening content in a controlled environment.

Keep Plugins and Add-ons Updated or Remove Them: Browser plugins like Flash or Java, as mentioned, should be uninstalled if possible. Most websites no longer need them. If you absolutely need Flash or others for some reason, set them to "Ask to activate" so they don't run automatically. Remove any unused browser extensions; only keep those you trust and need, since malicious or compromised extensions can hijack browsing.

Bookmarking Trusted Sites: Encourage using bookmarks/favorites for important sites (like your donation platform login, or government portals your CSO uses). This helps avoid typo squatting (accidentally going to yourbank-secure.com instead of yourbank.com). It also speeds up recognition – users click the known bookmark rather than retyping or googling the site each time (which could lead them astray).

Education on Pop-ups and Scams: No tool fully stops scams like "tech support" pop-ups that say, "You have a virus, call this number." So, maintain awareness: if any such pop-up occurs, or a download suddenly starts, close the browser or tab. Modern browsers block most pop-ups, but some ads simulate them. Using an ad-blocker mostly eliminates these. Also, modern operating systems have smarts: Windows 10's SmartScreen will often block known malicious downloads or warn you if an app isn't commonly downloaded.

By combining these tools and settings, everyday browsing becomes significantly safer. The goal is a layered defense – one extension might block a bad ad, the browser might warn of a deceptive site, and your caution does the rest. If something slips through, your antivirus might catch it on download. No single layer is foolproof, but together they greatly reduce risk.

Cloud Storage: Google Drive, Dropbox, and Their Security

Cloud storage services like Google Drive, Dropbox, Microsoft OneDrive, and others have revolutionized how CSOs collaborate and store data. They offer convenience and backup by default, but they also introduce security considerations. This section explains how to use these services securely.

Access Control and Sharing Settings: One of the biggest risks with cloud storage is accidental over-sharing. Always double-check how you share files or folders. By default, keep documents private to your organization or specific users. For example, Google Drive allows sharing to "Anyone with the link" – use that only when necessary and consider adding a password or expiry (Google doesn't offer a password on links, but OneDrive for Business and Dropbox do for paid accounts). Instead, prefer sharing with specific people's emails (they'll need to log in, which is more secure). Dropbox and Google both show icons indicating if a folder is shared – familiarize yourself with those indicators and audit them periodically. Google's **"Shared with me"** section and Dropbox's shared folder list can help review what's open.

If your CSO uses G Suite/Google Workspace or Microsoft 365, take advantage of administrative settings: you can restrict external sharing or at least monitor it. Perhaps limit who can share externally or set a default that

link sharing outside the organization is off. That way, an employee must intentionally override to share publicly. If you use a personal/free Google account, be extra careful, as those lack admin oversight, and one can inadvertently expose a file to the world.

Enable Two-Factor Authentication on Cloud Accounts: We have emphasized 2FA repeatedly, and it's critical for cloud storage since a breach of your account could expose a lot of data. Google, Dropbox, Microsoft, Box, etc., all support 2FA (usually via authenticator apps or SMS). Ensure every user in your team with access does this. Many breaches happen because login credentials get stolen, but 2FA would stop the attacker short.

Device Management and Remote Wipe: Use the options to manage devices. For example, Dropbox and OneDrive list all devices linked (computers, phones). If a device is lost or someone leaves, you can remotely unlink and, in Dropbox's case, even remotely wipe files that were set to local. Google Drive (Backup and Sync or the new Drive for desktop) doesn't quite wipe local files because they are usually just in a cache, but revoking access is still important. Google's admin panel (for Workspace) can wipe data from a user's Drive on a mobile device if you set up device management. Even if you can't auto-wipe, changing the password and signing out all sessions (usually an account security setting) helps ensure a lost laptop can't sync new data or the account can't be accessed.

Encryption of Sensitive Data: As mentioned earlier, while these services encrypt data on their servers, they do hold the keys (except for certain products like MEGA or SpiderOak, which are end-to-end encrypted but less commonly used). If you have particularly sensitive data you're putting in Google Drive or Dropbox, you might add your own layer of encryption. Options:

- Use tools like **VeraCrypt** to create an encrypted container and store that file on Drive/Dropbox. You then need VeraCrypt to open it with the password. Downsides: the whole container must resync when changed, and simultaneous collaboration inside it is not straightforward.

- Use **7-Zip** or **WinZip** to encrypt specific files before uploading if you plan to share them externally. Use a strong password and share that password via a different channel.
- Some cloud services offer an encrypted "vault" or "locker" as a feature (e.g., Dropbox Professional has a Vault). Know your tool's features.
- If using Office 365, you can apply sensitivity labels that encrypt files so only certain accounts can open them (this is a more advanced, enterprise feature, though).
- If using Google, avoid putting extremely sensitive content in Google Docs text unless necessary, since Google technically can access it. Perhaps use offline encrypted formats and just store them there, or use something like **Cryptomator** – a tool designed to encrypt files client-side before syncing to the cloud (it creates a virtual drive; files dropped in are encrypted and then synced). Cryptomator works well with Dropbox, Google Drive, etc., and doesn't require special server software (the cloud just sees gibberish files). For a CSO handling highly confidential info, that can be worth implementing for a subset of data.

Monitoring and Alerts: Some services allow activity monitoring. For instance, Dropbox shows a log of sharing events and logins on the account page. Google Workspace admin can set up alerts for things like "file shared externally" or "suspicious login attempt." If available, configure these. Even on personal accounts, Google Account Security will alert you of new device sign-ins – pay attention to those emails or prompts ("Did you just sign in from X device?").

Educate About Social Engineering: Attackers might not hack Google directly, but could phish you. An example: you get an email that appears to be a Google Drive share from a colleague, but it's actually a cleverly disguised phishing link that leads to a fake Google login. Google Drive phishing is a known tactic – because people trust the Drive/Docs share emails. So, verify unexpected shares before logging in via them. Google has improved by adding security scans to Docs, but caution is needed. Similarly,

don't enter your cloud password into any pop-up unexpectedly – better go to drive.google.com manually if prompted.

Version History and Ransomware Protection: One benefit of cloud storage is version history. If ransomware encrypts your local files and they sync to the cloud as gibberish, services like Dropbox and OneDrive keep older versions for some days. You could restore previous versions of many files (Dropbox Pro even has an extended version history option). Familiarize yourself with that process. OneDrive (business) also has a "Restore all files to a previous time" feature to recover en masse after a ransomware event. Know that it's there, but prevention is key to not needing it.

Using Organizational Accounts vs. Personal: If possible, use an organization-managed account for cloud storage rather than a bunch of personal accounts. For example, with Google Workspace for Nonprofits (which is often free/discounted for CSOs), you get managed accounts (like [name]@CSO.org) with Drive. That way, the data can be owned by the organization, and you can control it if someone leaves. Personal accounts tie data to individuals, which can be messy if the person moves on. Also, Google Workspace and Microsoft 365 for organizations have better security controls by design than free accounts. Look into those nonprofit offers (Google for Nonprofits, Microsoft for Nonprofits), as they can boost security (and collaboration) significantly at low or no cost.

Regular Audits: Take time, perhaps quarterly or biannually, to audit your cloud drives. Remove old data you no longer need (reduces exposure). Check sharing settings on critical folders. Remove access for users who no longer require it. This maintenance ensures your cloud environment stays tidy and secure.

In summary, services like Google Drive and Dropbox can be safe for CSOs if used wisely: protect accounts with strong authentication, configure sharing thoughtfully, and perhaps add extra encryption for highly sensitive files. The convenience and collaboration benefits are huge, so it's mostly about using the tools' security features to their fullest. Most incidents on these platforms happen due to human error (like sharing a link publicly by

mistake or using a weak password) rather than the providers being breached. By addressing those human factors and technical settings, you can confidently leverage the cloud.

Protecting Your Phone and Computer

In earlier sections, we discussed general device security practices. Here, we'll get into some specific tools and settings to further secure your computers and mobile devices, since they are the endpoints where you access all your digital resources.

Ensure FDE is enabled on all laptops and mobile devices. On modern computers, this often requires just turning it on:

- Windows 10/11: Use **BitLocker** (on Pro editions) or the Device Encryption in Home (if available). Once turned on, it encrypts the whole drive and ties decryption to your password/PIN (and TPM chip). BitLocker can also encrypt USB drives (you can use BitLocker To Go for that).
- macOS: Turn on **FileVault** in Security settings; it's a one-click to encrypt the Mac's disk.
- Linux: If using Linux, install with LUKS encryption enabled or use a tool like cryptsetup. Many user-friendly distros allow enabling encryption during installation.
- Android: Most modern Android devices encrypt storage by default (especially since Android 7.0+). Just make sure you set a strong PIN/password/pattern, because encryption is only as strong as the lock screen.
- iPhones/iPads: They are automatically hardware-encrypted as long as you set a passcode. So always use a passcode (and Touch/Face ID for convenience, but that's locked to the passcode as backup).

Mobile Device Security Apps: For Android, consider installing a reputable security app. Options: **Google Play Protect** is built-in and scans apps (make sure that's enabled in Play Store settings). Third-party AV like **Avast Mobile**, **Bitdefender Mobile**, or **Lookout** can add phishing protection and find-my-phone features. They can also scan for malicious apps beyond what Play

Protect finds (though Google's is decent). For iOS, separate security apps are less needed due to sandboxing (though apps like Lookout can help with phone locating or checking if your iOS is jailbroken).

***Find My Device*:** Always enable find-and-remote-wipe services:

- Android: Use **Find My Device** (a Google service) – it's usually on if you have a Google account on the phone. Test it (Google "find my device" and see if your phone is found).
- Samsung devices also have **Find My Mobile,** which can be an alternative with more features.
- iPhone: Ensure **Find My iPhone** is on (in iCloud settings). This allows you to locate or erase a lost phone.
- Laptops: Consider a laptop tracking software if theft is a concern. PreyProject (Prey) has a free plan for up to three devices and can help locate a lost/stolen laptop and even take pictures or send messages. Some business laptops have anti-theft built in (like Computrace/LoJack). But even without specialized software, if a laptop is lost, immediately change passwords for accounts it had access to, and if it was encrypted, you at least know the data is safe.

Firewall on Computers: Windows Firewall is on by default – keep it on. It silently does its job, blocking unsolicited inbound traffic. You can also use it to block specific apps from outbound if needed (less common for CSO scenario). On Mac, turn on the firewall in Security preferences. You likely don't need third-party firewall software; built-in ones are fine and avoid confusing prompts that less tech-savvy might just allow anyway.

Firmware and BIOS Security: For high-security needs, consider setting a BIOS/UEFI password on laptops (so that booting from external media or altering boot settings requires a password). Also enable Secure Boot (to prevent rootkits). These steps prevent an attacker with physical access from, say, booting a live OS to bypass your system security. That said, if you have FDE and a strong password, they shouldn't get in anyway. But a BIOS password adds a layer against tampering or using the machine.

Device Updates Automation: We talked OS updates; additionally:

- Keep apps updated, e.g., ensure Microsoft Office or LibreOffice is up-to-date (Office usually auto-updates via Office 365 if you have that, otherwise check Windows Update or Office's update).
- PDF reader: If using Acrobat Reader, update it. Or use a safer reader like **SumatraPDF** or your browser's PDF viewer, which are simpler and less exploited.
- Java: If you must have it, set it to update automatically. If you don't need it, uninstall it entirely.
- On phones, update apps via Play Store/App Store whenever updates are available (enable auto-update on Wi-Fi to make it effortless).

Disable Unnecessary Features: Unused open doors can be closed:

- On Windows, if you don't need features like RDP (Remote Desktop) or file sharing, turn them off to reduce the attack surface.
- On phones, be mindful of Bluetooth and NFC – keep them off when not in use (Bluetooth attacks are less common now with patches, but it's still good hygiene, especially in public spaces).
- Remove bloatware apps on phones that you don't use, especially ones that might run in the background or have permissions (some Android phones come with preinstalled apps that could be data-mining).
- On any system, don't log in as an administrator for daily use. Have a standard user account for routine work and an admin account for installing software. This way, if malware runs, it might not have admin rights to do deep changes. Admittedly, many people ignore this, but it is a recommended practice on Windows and Linux. On Mac, the initial user is admin, but Mac will prompt for password escalation, which acts similarly to separating privileges.

Use a Good Security Software Suite: If budget allows or free options suffice, use a well-rounded security suite. For example, **Microsoft Defender** actually includes not just anti-malware but also Controlled Folder Access (ransomware protection that stops unknown apps from editing your documents), and cloud-based protection if turned on. Third-party suites

might include a password manager, VPN trial, etc. Only invest if you need those extras; otherwise, layered individual tools work.

Email Security on Device: If using an email client like Outlook or Thunderbird, ensure it is updated. Be cautious with what attachments you open. Modern email clients have some sandboxing (Outlook, for instance, won't load images or run macros by default, and warns if an app tries to access email data). Don't enable "allow programmatic access" unless needed by some integration.

Physical Protections: Laptops – consider using a Kensington lock cable if you leave it in a shared space (to deter opportunistic theft). For phones, use protective cases and perhaps privacy screen protectors if you handle sensitive info on them in public (prevents shoulder-surfing).

Data Backups for Devices: We talked about backups, but one aspect: for mobile devices, back up your data as well (cloud backup or manual). For iPhones, use iCloud or local iTunes backups; for Android, use Google's backup services or apps for critical data. That way, a lost device doesn't mean lost data, and you can remotely wipe without hesitation, knowing it's saved.

Anti-Theft Labeling: Sometimes the simplest solutions are the best: Label your devices with contact info. A person finding a lost device might return it if easy (like a sticker saying "If found, call [CSO number]"). This is more of a recovery tip than security, but it can save the day.

Plan for Device Replacement: Have a simple plan if a device is compromised or outdated. For example, if a computer no longer receives updates (Windows 7, old Android), phase it out or isolate it from sensitive tasks. Maybe use it offline if necessary for something legacy. But do invest in keeping hardware within supported life for security.

By using the above methods and tools on your phones and computers, you create a strong defensive perimeter around your personal and work data. Think of your device as a secure vault: you've locked it (strong login), alarmed it (antivirus and firewall), reinforced it (updates and encryption), and set up a way to locate or destroy contents if it's taken (find my device,

remote wipe). With such measures, even if threats arise, you either block them or are prepared to respond without catastrophic loss.

This concludes the chapter on tools. By adopting secure applications (4.1), practicing safe browsing (4.2), properly using cloud storage (4.3), and fortifying devices (4.4), your CSO will have a much stronger digital security posture. Next, we'll discuss what to do if, despite all this, a cyberissue occurs – because no defense is 100% perfect, having a response plan is vital.

Chapter Summary

Chapter 4 focuses on securing the technology CSOs rely on, including computers, networks, and websites. It recommends keeping software updated to patch vulnerabilities, using antivirus tools (e.g., Avast Free) to combat malware, and securing Wi-Fi with WPA2/WPA3 encryption. For websites, it advises enabling HTTPS, regular backups, and updating Content Management Systems (e.g., WordPress) to prevent defacement or DDoS attacks. A case study of a CSO's website redirecting to a third-party site due to outdated software illustrates the risks. The chapter promotes VPNs (e.g., ProtonVPN) for secure connections on public Wi-Fi, vital for field staff. It emphasizes low-cost solutions, like free HTTPS via Let's Encrypt, to suit CSO budgets. Non-technical staff are guided to verify settings (e.g., checking for HTTPS padlocks) without needing IT expertise. The chapter also covers device encryption and strong passwords to protect against theft or loss. By securing infrastructure, CSOs prevent disruptions and data breaches, ensuring mission continuity. The chapter's practical steps, like scheduling automatic updates, make implementation straightforward, aligning with the e-book's goal of accessible cybersecurity.

Social Media Account Security Checklist for CSOs

This checklist helps CSOs secure their social media accounts (e.g., Twitter/X, Facebook, Instagram) to protect their online presence and reputation from hijacking, misinformation, or unauthorized access. These steps are designed for program staff and volunteers with minimal technical expertise to complete in one or two hours. Work through each item, checking off completed tasks. If you're unsure, ask your social media manager, IT contact, or platform support for help. Share findings with your team to maintain a secure online presence.

1. Enable Two-Factor Authentication (2FA)

- Turn on 2FA for all social media accounts to require a second verification step (e.g., a code sent to your phone or app).
- Platform Tips:
  - » Twitter/X: Go to Settings > Privacy and Security > Two-Factor Authentication. Choose an authenticator app (e.g., Google Authenticator) or SMS.
  - » Facebook: Navigate to Settings > Security and Login > Two-Factor Authentication. Select an authenticator app or text message.
  - » Instagram: Go to Settings > Security > Two-Factor Authentication. Enable app-based or SMS authentication.
- Example: A hacked CSO Twitter account posted false messages. 2FA prevented further unauthorized access.
- Log into each account, enable 2FA, and test it with your team's devices.

2. Use Strong, Unique Passwords

- Update passwords to at least 14 characters, mixing letters, numbers, and symbols (e.g., "sunbird&glass7rain"). Use a different password for each account.
- Consider a free password manager (e.g., Bitwarden) to store passwords securely.
- Platform Tips:

» Twitter/X: Update in Settings > Change Password. Avoid reusing passwords from other platforms.

» Facebook: Go to Settings > Security and Login > Change Password. Ensure it's unique from email or other accounts.

» Instagram: Navigate to Settings > Security > Password. Use a passphrase for easier recall.

• Example: a CSO's Instagram was compromised due to a reused email password. A unique password fixed the issue.

• Change passwords for all accounts and store them in a password manager.

3. Remove Unused Admin Accounts

• Check who has admin or editor access to your social media accounts and remove former staff, volunteers, or inactive users.

• Platform Tips:

» Twitter/X: Go to Settings > Creator Subscriptions > Manage Team to review and remove admins.

» Facebook: Navigate to Page Settings > Page Roles to see and delete unnecessary admins or editors.

» Instagram: Check Settings > Authorized Apps or Business Settings > Users to revoke access for unused accounts.

• Example: A former volunteer's admin access was used to post unauthorized content. Removing old admins prevented recurrence.

• Ask your social media manager: "Can we review and remove outdated admin accounts?"

4. Set Up and Verify Recovery Email/Phone

• Ensure each account has a current recovery email or phone number controlled by trusted staff for account recovery if locked out or hacked.

• Platform Tips:

» Twitter/X: Update in Settings > Your Account > Account Information. Verify the recovery email is active.

» Facebook: Go to Settings > Security and Login > Contact to add or update a recovery email/phone.

» Instagram: Navigate to Settings > Security > Account Recovery to confirm a valid email or phone.

• Example: a CSO regained a hacked Facebook account using a recovery email. Without it, recovery took weeks.

• Add or update recovery details and test by requesting a recovery code.

5. Monitor Account Activity

• Regularly check for unusual activity (e.g., posts you didn't create, logins from unknown locations).

• Enable login alerts where available to get notifications of suspicious activity.

• Platform Tips:

» Twitter/X: Check Settings > Privacy and Security > Connected Accounts for unfamiliar devices or apps.

» Facebook: Go to Settings > Security and Login > Where You're Logged In to review active sessions. Enable login alerts.

» Instagram: Navigate to Settings > Security > Login Activity to see login locations and enable notifications.

• Example: a CSO spotted a login from another country and locked the account before damage was done.

• Review activity logs weekly and report odd behavior to platform support.

6. Limit Third-Party App Access

• Remove access for third-party apps or tools (e.g., scheduling tools, analytics apps) no longer used or untrusted.

• Platform Tips:

» Twitter/X: Go to Settings > Privacy and Security > Connected Accounts to revoke app permissions.

» Facebook: Navigate to Settings > Apps and Websites to remove unused or suspicious apps.

» Instagram: Check Settings > Security > Apps and Websites to revoke access for unneeded apps.

• Example: A scheduling app with outdated access was used to post spam on a CSO's Twitter. Revoking access fixed it.

• Review and remove unnecessary app connections in account settings.

7. Train Staff on Safe Social Media Use

• Remind staff and volunteers not to share account credentials, click suspicious links, or post sensitive data (e.g., donor info) on social media.

• Share a tip: "Log out of accounts on shared or public devices."

• Þ Example: A volunteer posted sensitive campaign details on a public Instagram post. Training prevented future errors.

• Send a team email: "Never share social media logins. Log out after use on shared devices."

8. Plan for Misinformation or Hijacking

• Develop a simple response plan for hacked accounts or misinformation (e.g., platform report, post a clarification to followers).

• Keep a draft statement ready: "Our account was compromised. Please ignore recent posts. We're resolving this."

• Platform Tips:

» Twitter/X: Report hacks via help.twitter.com/forms/security.

» Facebook: Use facebook.com/hacked to report compromised accounts.

» Instagram: Report issues via Settings > Help > Report a Hacked Account.

• Example: a CSO quickly clarified a hacked post on Facebook, reducing misinformation spread.

• Draft a response statement and save platform support links for quick access.

2.5 CHAPTER

5: SAMPLE CYBERSECURITY INCIDENT SCENARIOS

What to Do if You Experience a Cyberincident

Despite best efforts at prevention, incidents can still happen. A quick, calm, and methodical response can significantly reduce the harm caused by a cyberincident. This chapter guides you through recognizing signs of an incident, immediate steps to take, whom to contact for help, and how to restore security afterwards. Essentially, it's your emergency action plan for the digital realm.

Recognizing the Signs of a Cyberattack

The sooner you realize something is wrong, the faster you can respond. Cyberattacks can manifest in various ways; some obvious, some subtle. Here are common red flags that may indicate a problem:

Ransomware Message or Locked Screen: A very clear sign – your computer suddenly displays a message that your files are encrypted or demands a ransom to unlock your system. You may be unable to open files, and they might have strange extensions. Often, the background might change to instructions, or a window pops up listing files and payment instructions. If you see this, it's almost certainly a ransomware attack.

Antivirus Warnings or Fake AV Pop-ups: If your antivirus catches something, take it seriously. Conversely, if you see a rogue pop-up claiming "Your computer is infected! Click here to scan," and it's not from your AV but a website, that is a tactic to lure you into installing malware. Recognize the difference: your actual AV software will have its familiar interface and likely won't prompt via a random browser ad.

Unexpected Toolbars or Browser Behavior: Suddenly, your browser has new toolbars, or your homepage/search engine changed without your input, or searches redirect to odd sites. This suggests adware or malware has been installed. Similarly, frequent pop-up ads when you're offline or on sites that normally don't show them can indicate an infection.

Unfamiliar Programs or Processes: You notice an application you never installed. Or your computer's fan is running high, and it's slow, and Task Manager/Activity Monitor shows unknown processes hogging CPU. Some malware might run invisibly, but many will consume resources (like cryptominers, making your system sluggish). If you see a program open briefly, then disappear, or new icons on the desktop, investigate.

Your Friends Receive Odd Messages from You: If colleagues or friends say they got a strange email or social media message from you that you didn't send, your account might be compromised. Examples: spam emails from your address, or your WhatsApp sending a suspicious link in group chats. This is a sign that either your device or that account was taken over.

Password Not Working: A very alarming sign is if you suddenly cannot log into an account because the password was changed (and you didn't change it). If your known correct password is rejected and the account recovery indicates a change, assume a breach of that account.

Unusual Network or System Activity: This can be harder to notice for an average user, but if you have a network monitor tool or IT admin: examples are a surge in outbound traffic, unknown devices on the network, or the hard drive light blinks constantly when you're not doing anything (could mean data is being exfiltrated or a virus scanning your files). Also check firewall alerts (if any) or Windows Defender logs for repeated blocked actions.

Files Missing or Altered: If you find that files are deleted or content changed without explanation, that's concerning. Data could be being wiped or tampered with by an attacker. Also, if you see files that have garbled names or extensions like locked or encrypted, that's indicative of ransomware.

Strange Cursor or Control: In extreme cases, if your mouse moves on its own or windows open and you're not doing it, someone may have remote control (as if remote desktop or RAT malware is operating). Disconnect from the internet immediately if this happens.

System Warnings or Crash Screens: Repeated crashes or blue screens could just be hardware/software issues, but sometimes rootkits or deep malware cause instability. If it started happening along with other signs, consider malware as a possibility.

Browser Redirections: If, when you try to visit common sites (like a bank or Gmail), you consistently get redirected to a slightly different URL or see certificate warnings unexpectedly, you might have malware or a DNS hijack. For instance, trying to go to facebook.com but always landing on a page that doesn't look right means trouble.

In practice, many of these signs overlap. For example, a ransomware attack will produce encrypted files (which you can't open), possibly a ransom note text file in each folder, and maybe a changed desktop wallpaper announcing it. Phishing account compromises often are discovered when others inform you of weird messages or when you get login alerts from unusual places.

If you suspect an issue but aren't sure, err on the side of caution:

- If it's a potential virus, run a full antivirus scan.
- If an account might be compromised, try logging in from a different secure device and change the password if you still can, or see account activity logs.
- Keep an eye on network usage (on Windows 10, you can see network usage per app in Task Manager, too).
- If your device has a diagnostic or security scan tool (like Windows Security or a third-party), use it.

The key is to stay vigilant. One CSO practice is to encourage staff to speak up if "their computer is acting strange." It's better to investigate false alarms than to miss a real breach. Don't let potential stigma stop reporting; in security training, emphasize that timely reporting is critical, and they won't be blamed for raising a concern.

Now that you know what to look for, the next step is to act promptly when something seems wrong. The following sections will cover immediate response steps, who to call for help, and how to recover.

Step-by-Step Response: What to Do When Something Goes Wrong

The moment you realize a cyberincident might be happening, it's crucial to take deliberate steps to contain and investigate the issue. Panicking or doing the wrong thing (like immediately paying a ransom or deleting evidence) can make matters worse. Here is a step-by-step guide that aligns with standard incident response phases (identify, contain, eradicate, recover) in simplified terms for a CSO environment:

1. Don't Panic, Assess the Situation: Take a breath and try to understand what's happening. What are the signs and scope? For instance, is it one computer behaving oddly or multiple? Is it an account issue or a device issue? Identifying the nature of the incident guides the next steps. Jot down what you observed (time, symptoms). If needed, quickly take photos or screenshots of suspicious messages or error screens with your phone (useful for evidence and asking experts later).

2. Disconnect Affected Systems: If you suspect active malware, especially if data might be being stolen or if more systems are infected, isolate the machine from the network immediately. Unplug the Ethernet cable or turn off Wi-Fi. This prevents spread (e.g., some worms or ransomware try to jump to network drives) and stops an attacker's remote control or data exfiltration. However, do not power off the system unless you have to – simply disconnect the network. There is nuance: powering off stops malware but also can erase volatile evidence. For most CSO scenarios, it's okay to leave it on and disconnected, then run scans. But if ransomware is actively encrypting files in front of your eyes, you might quickly power off to halt it. Use judgment; when in doubt, network off is a good first move.

3. Secure Your Accounts: If an account is compromised (like email or social media), **try to regain control**. Use account recovery flows: reset passwords immediately. Sign out all active sessions (many services have a "log out of all devices" function). Enable 2FA if not already (even if the hacker still has a session, once you kick them out, 2FA will help stop re-login). Notify colleagues that the account was compromised, so they should treat any recent messages as potentially fraudulent. If you cannot regain

access (hacker changed the password and locked you out), contact the service provider's support right away to report an account takeover.

4. Inform the Person in Charge (and Possibly Everyone): As per your security plan (from Chapter 3), you should have a point person or team for incidents. Inform them immediately. If you are that person, gather relevant people. For example, if a shared server is hit, alert all users not to use it until further notice. If one employee's PC is infected, you might caution others not to open emails from that PC, etc. **Do not keep an incident secret** – hiding it can worsen damage. Quick communication allows others to be vigilant or take protective steps (like changing their passwords if needed). Also, if you have IT support (in-house or contracted), call them early. They can start assisting with tech measures or deeper analysis.

5. Contain the Damage: Beyond disconnecting the network, here are containment steps:

- If it's malware on a PC, run an antivirus scan in safe mode, if possible, or using a bootable rescue disk. This can quarantine the malware, stopping further harm. However, contain first (network off), then scan – don't run scans while still online if an active attacker might be watching or additional payloads could download.
- If it's ransomware and files are encrypted, identify if it has stopped or is still running. Kill suspicious processes via Task Manager if you see them (some use obvious names, others are random). But at this stage, likely the encryption is done quickly. Containment then means quarantining that PC and not touching files (so forensic experts or decryption tools might attempt recovery).
- If a website is under attack (defaced or hacked), take it offline if you can (e.g., put up a maintenance page or ask the host to temporarily suspend) to prevent further damage to visitors and give you time to fix.
- For email breaches, besides changing the password, consider emailing contacts to warn them of potential phishing that came from your account.

- If data was leaked (like you find your database on a paste site), restrict access to those systems until you understand the exploit path and patch it.

6. Document Everything: As you do the above, keep notes. Write down times, actions you took, and who is notified. If you find a suspicious file or process name, note it. This documentation helps later for recovery, reporting, and improving your security plan. It's also useful if you involve law enforcement or an incident response professional; they'll want to know the sequence of events.

7. Seek Assistance if Needed: Don't hesitate to get outside help. If you have a cybersecurity contact (perhaps another CSO's IT, a volunteer expert, or a cybersecurity helpline), call them. Many countries also have CERTs (Computer Emergency Response Teams) that might assist or advise even small organizations. There are also free community resources; for example, in a ransomware case, you could check the website "No More Ransom" to see if a decryption tool exists for your strain. But apply only reputable tools – for any online advice, ensure it's legitimate. If unsure, ask your trusted IT advisors.

8. Preserve Evidence (Especially for Serious Incidents): If the incident might involve crime (e.g., a deliberate hack, significant theft), you may later involve law enforcement. In such cases, preserving logs and evidence is crucial. Avoid deleting system logs or wiping the system until the issue is understood and resolved. If you have to rebuild a system, consider making an image of the disk first. In less critical cases, evidence is still useful for learning – e.g., keep the phishing email that fooled someone, to study it and educate others.

9. Eradicate the Threat: Once contained, work on removal. For malware: use AV to remove it fully, or in stubborn cases, reformat/reinstall the OS (starting fresh is the surest way if you have backups and it's not too onerous). For compromised accounts: double-check no backdoors (like ensure in email no new forwarding rules were set by the attacker to secretly forward mails, an often-overlooked trick). Check other accounts because sometimes

one cred gets many – for instance, if the browser saved passwords, an attacker might grab them, so you might need to change other accounts' passwords too.

If the incident was a vulnerability (like your website had an outdated plugin that got exploited), patch or remove that. If a rogue insider was the problem, obviously, remove their access.

10. Recover and Restore: After eliminating the immediate threat, begin getting back to normal:

- Restore lost or corrupted data from backups. Verify that backups are clean (scan them with AV before restoring if possible).
- Reconnect systems carefully. For example, after cleaning a PC, bring it back on the network and monitor if any suspicious outbound traffic resumes (if it does, maybe the malware wasn't fully gone).
- If you re-enabled accounts or changed credentials, make sure everyone can access what they need again, with new secure passwords.
- If operations were halted (like you took a server offline), coordinate to bring it up during off-peak to test, ensuring no residual compromise.

11. Communicate Updates: Keep staff informed of what happened and what is being done. Transparency builds trust and cooperation. Also, if relevant, inform external stakeholders as appropriate (see next section on who to contact, e.g., donors if their data was breached, etc.). However, generally, internal issues can be kept internal unless there's a need or duty to report externally.

Throughout this process, maintain an attitude of learning, not blame. Attacks happen to the best of us. Focus on resolution and preventing a recurrence rather than dwelling on who clicked what (aside from using that info to improve training).

This structured response – identify, contain, eradicate, recover – mirrors guidance from experts. For small CSOs, the steps might be done by one person wearing many hats, but the principle remains.

Next, let's examine in more detail who you might need to call or report to, because handling an incident can involve more parties than just your

organization.

Who to Turn to for Help: Support Resources and Getting Assistance

When dealing with a cyberincident, you don't have to handle it all alone. There are several places and people you can reach out to for help, advice, and reporting. Here's a breakdown of support resources:

Internal Team and IT Support: First, within your organization, involve anyone responsible for IT or security (your "techie" staff/volunteer, or the person who set up your systems). If you have an IT managed service provider or a volunteer IT advisor, contact them immediately and describe the situation. They likely have seen similar issues and can guide technical steps. Even a tech-savvy board member or partner organization's IT person can be a valuable ally in a pinch.

Peer Networks and Other CSOs: Consider reaching out discreetly to sister organizations or networks. Often, CSO networks (for example, a human rights network or a CSO umbrella organization) might have shared resources or at least collective knowledge. They might know of common threats in your sector or region and have recommendations (like "Yes, two other CSOs got that same phishing email; here's what we did"). Collaboration can be powerful here. However, weigh how much detail to share externally – keep sensitive specifics for trusted contacts to avoid any reputational risk until official.

Cybersecurity Helplines for Civil Society: There are initiatives specifically to help civil society with digital security emergencies. A notable one is **Access Now's Digital Security Helpline**, which provides 24/7 free assistance to CSOs, activists, and journalists worldwide. They can help in cases like website attacks, account compromises, etc., often bridging to expert volunteers or giving tailored guidance. If you find yourself in a serious situation beyond your capacity, don't hesitate to email or call such a helpline (Access Now's is ). They maintain confidentiality and are used to handling urgent cases.

Another example: **CyberPeace Institute's CyberPeace Builders** program offers free cybersecurity assistance by corporate volunteers to CSOs. If

you're already enrolled or connected to them, use that channel. If not, maybe something to consider for the future.

Law Enforcement: This depends on the nature of the incident:

- If it's a significant data breach involving theft of personal data or a deliberate hack, you might consider informing local law enforcement or a cybercrime unit. They can investigate, especially if donors' money or sensitive info was stolen, or if there's extortion (like ransomware demands). However, experiences vary – in some places, police are helpful; in others, they may not prioritize or have expertise.
- In countries with mandatory breach notification laws (like under GDPR in the EU, serious personal data breaches must be reported to data protection authorities within 72 hours), you should follow those regulations. That means informing the relevant Data Protection Authority, if applicable, and possibly affected individuals (more on that in the next section).
- If you suspect the attacker is from a specific region or there's a pattern affecting multiple organizations, law enforcement might piece these together.
- Note: If your CSO works on sensitive issues in a country where authorities might not be friendly or might misuse that info (for instance, if the attack could be state-sponsored), you'll have to carefully weigh engaging law enforcement. In such cases, consulting international bodies (like maybe a CERT in a neutral country or just using CSO helplines) might be preferred initially.

National CERT/CSIRT: Many countries have a Computer Emergency Response Team (CERT) or CSIRT, often under a gov or academic umbrella. They sometimes assist organizations (not just critical infrastructure). Some have special arms for small businesses or nonprofits. For example, **CERTs in the EU** often respond to incidents and can give advice or coordinate with law enforcement. If you have a contact or can easily report via their website, it might be beneficial. They also might warn others or track the spread of a malware campaign.

Donors or Partners: If a project or donor data is involved, or if service delivery is impacted, you might need to inform partners. For instance, if you run a joint project and hackers deface the project website, telling the partner from the other CSO ensures they're aware and can help, or at least are not caught off guard. Donors might have reporting requirements if funds are affected (say, financial fraud). On the supportive side, some donors (particularly larger ones or those funding cybersecurity capacity) might have resources to help you. But manage communication carefully – focus on what is being done to fix it, not just the problem, to maintain confidence.

Insurance: If you have cyber insurance or general liability that covers cyberincidents, notify the insurer's incident hotline as soon as possible (often required for coverage). They can dispatch professional incident responders or guide next steps. Many insurance policies require insurer coordination for things like paying ransom decisions. If you don't have insurance, this doesn't apply, obviously.

Community and Online Resources: There are online forums like the **Reddit r/cybersecurity or r/techsupport** or **StackExchange Security** where professionals sometimes assist. But be cautious not to divulge sensitive details in public forums. Instead, one might search those forums to see if others have dealt with the specific malware or error (often someone has posted about that specific ransom note or virus behavior, which can give clues on fixes). Websites like **BleepingComputer** have dedicated sections for help with malware removal and specific ransomware support threads, often moderated by experts who help victims for free. They often collaborate with the NoMoreRansom project, too. If you go that route, follow their guidelines (they often request posting log files, etc. – but don't do anything you're not comfortable with; perhaps use a pseudonym if discussing your case publicly).

When and How to Inform Affected Individuals/Public: This is more of a "who to notify" as well: if personal data of beneficiaries or stakeholders is leaked, ethical and possibly legal duty might compel you to inform those individuals so they can protect themselves (e.g., change their passwords if

their email was leaked, watch for identity theft). Crafting such communications can be tricky; it should be honest, apologetic, and provide guidance (like "We experienced a security incident where your email address might have been exposed. Be vigilant for suspicious emails and consider changing your password if you reused it …"). If you're unsure, consult a communications or legal advisor – you want to strike the right tone and not inadvertently admit liability incorrectly, etc.

Psychological Support: This might sound off-topic, but a serious incident can be stressful. People might feel violated or guilty (the person who clicked on phishing could feel awful). It's worth addressing morale. Ensure everyone knows that mistakes happen and focus on moving forward. If extremely stressed, maybe take a short break or get someone to talk to (even venting to a colleague in another CSO who went through a similar experience can be reassuring). After things settle, consider a debrief session that's supportive: discuss what happened and how to help each other cope and strengthen.

In all communications with outside entities, keep records of who you contacted and when, and any case/reference numbers or advice given. This is part of the documentation and helps with follow-up.

Finally, use these support channels not only during an incident but afterwards to improve. For example, the Access Now helpline could advise what steps to take in the future to avoid repeats, or CERT might send you their report and recommendations.

Restoring Security: Steps to Recovery

After containing the incident and getting help, the final phase is to bring systems back to normal operation and implement measures to prevent a recurrence. Recovery isn't just about restoring data, but also about restoring confidence that your environment is clean and secure again.

Clean and Rebuild Systems: If any machines were infected, after removal of malware, evaluate if a full OS reinstall is warranted. Often, security experts suggest that for serious compromises (like rootkits or unknown malware), a wipe and rebuild is the safest way to be sure the system is clean. Yes, it's

time-consuming to reinstall apps and restore files, but it gives peace of mind that no hidden backdoor remains. If you choose not to, at least run multiple scanning tools (one AV might miss something another catches). Tools like Malwarebytes, HitmanPro, etc., can be run in addition to your main AV for a second opinion. Ensure the OS is patched fully after cleaning.

For accounts, after regaining access, review account settings: Did the attacker set up any forwarding rules, add recovery emails, or 2FA devices of their own? (This is common: e.g., a Gmail hacker might add their email as a recovery email, so even after a password change, they try account recovery.) Remove any such unauthorized changes. Check mail filters, app passwords, connected apps – basically anything in account settings that could allow continued access.

If a website was hacked, after fixing the vulnerability and restoring content, consider moving it to a more secure host or adding a web application firewall (WAF). Possibly do a security audit of the code if it's a custom site. Also, change all database and FTP passwords in case they were compromised.

Restore Data from Backups: Bring back any lost data. For instance, if you had to wipe a PC, retrieve its user files from the backup (but scan them first, just in case an infected file was lurking in documents). If a database was wiped or encrypted, recover the latest backup. Test that the restored data is intact and the systems using it work properly. Sometimes backups aren't as fresh as we'd like, so you may lose a little work. After recovery, have staff quickly check if anything is missing from the gap, and if so, see if it can be re-entered or re-collected.

If ransomware was involved and you have no backups, the recovery is tougher. Consult experts or NoMoreRansom for decryption tools – sometimes free solutions exist for certain ransomware strains. Paying ransom is generally discouraged (it funds criminals and no guarantee), but some organizations make that tough choice. Engage law enforcement before paying, as they sometimes have keys or can advise. If ultimately there's data

loss, plan how to rebuild that data (maybe contacting partners to send you copies of files they have, etc.).

Improve and Update Security Measures: After a breach, one must harden defenses. This is the "lessons learned" phase, where you patch the holes that were exploited:

- If it was phishing, clearly more training and perhaps technical controls (like a better spam filter or an MFA enforcement) are needed. For example, enforce that all email accounts have 2FA enabled and maybe implement an email warning for external senders (some systems put "[External]" in the subject if mail came from outside, to help spot spoofing).
- If it was a weak password or reused credential, step up password policies (longer, unique) and consider using a password manager organization-wide to aid that. And definitely 2FA on everything critical.
- If malware came via unpatched software, ensure updates are applied more promptly. Maybe use a tool to monitor missing patches or subscribe to security bulletins relevant to your software.
- If a certain service was exposed (like an open RDP port that got brute-forced), close it or put it behind a VPN.
- Check that your firewall rules are tightened, unnecessary services disabled (as we covered in 4.4).
- Consider segmenting your network or data: e.g., in the future keep backups on a device not always connected so ransomware can't hit them, or separate sensitive data to a drive that not everyone can access.
- Implement better monitoring: perhaps enable system logging and set up alerts (there are free log monitoring tools or even just Windows Event Forwarding to watch for certain events like multiple failed logins).
- Plan a formal incident response procedure if you didn't have one – basically writing down what you did this time and improving it for next time (part of security plan updates).

Communicate to Stakeholders: If you had to notify people of the incident, follow up once resolved. For example, let your board or donors know, "We

experienced X, we took steps Y, and now operations are restored. We are implementing Z to ensure this doesn't happen again." This reassurance and accountability can strengthen trust if done transparently and competently. Likewise, if volunteers or beneficiaries were informed earlier to be cautious, later inform them the issue is resolved: e.g., "Our website is now secure and back online. Thank you for your patience."

Psychological Recovery: After a breach, team morale might be hit. People might feel uneasy ("Are we sure hackers aren't still in?") or guilty. Have a debrief meeting to discuss openly what happened and treat it as a learning opportunity rather than a witch-hunt. Commend the swift reporting or actions that limited damage. Maybe have a small 'lessons learned' workshop where you update everyone on what new measures are in place, which will also reassure them that things are safer now. The tone should be: we faced a challenge and overcame it, now we're stronger.

Documentation and Reporting: Write an internal report on the incident – even if just a page. Document timeline, root cause (if known), actions taken, and recommendations. This is useful for memory (six months later, you might forget details that matter if something similar happens) and for any external reporting duties. If required by regulation (e.g., GDPR), file that formal report to the authority, including those details. If you coordinate with an umbrella organization or have an obligation to donors (some grants require reporting serious events as part of risk management), use the internal report to communicate appropriately.

Test and Update Plans: Once everything is normal, it's a perfect time to refine your security plan and incident response. Update your contact lists (maybe you realized you didn't have the CERT's number handy – now save it). If a particular tool would have helped detect or stop it sooner, consider implementing that. Even consider conducting a small "fire drill" in the future – for example, test restoring backups or have a simulated phishing test to see if new training sticks.

Remember that **full recovery includes regaining trust**. Trust of your staff in the systems, trust of external partners in your handling. Transparency,

action, and follow-up help rebuild that trust. It shows you took it seriously and improved.

Finally, it's worth sharing knowledge (without sensitive details) with the community if appropriate. For instance, if you discovered a new scam targeting CSOs, warning others via a mailing list or network can prevent them from falling victim – a positive outcome from your ordeal.

By meticulously going through these recovery steps, you not only restore normalcy but ideally emerge with a more robust security posture. Many organizations find that a breach was a wake-up call that ultimately left them better prepared for the future (though it's always better to improve without the pain of an incident!).

At this point, we've covered how to handle incidents themselves. Next, we'll move on to the power of collaboration and community in staying secure, which is an often-underutilized aspect of cybersecurity for civil society.

Chapter Summary

This chapter emphasizes the human side of cybersecurity, advocating for a security-aware culture through training and policies. It highlights that 74% of breaches involve human error, such as phishing, making staff education critical. CSOs are guided to conduct basic cybersecurity training, covering password management and spotting phishing emails, using exercises like phishing quizzes. The chapter provides advice on drafting acceptable use policies for devices and data, ensuring clear rules for staff and volunteers. It also outlines protocols for incident reporting, encouraging prompt communication to contain breaches. Examples include a CSO training staff to report suspicious emails, preventing a malware attack. The chapter stresses leadership's role in modeling secure practices (e.g., using 2FA) to legitimize efforts. It recommends rewarding vigilance, like praising staff for reporting phishing, to reinforce habits. By embedding security into daily workflows, CSOs create a resilient culture. The chapter's focus on simple, inclusive practices ensures accessibility for all staff, aligning with the curriculum's train-the-trainer model and the e-book's goal of fostering long-term security habits.

Non-Technical Website Security Checklist for CSOs

This checklist empowers program staff and volunteers to verify and improve your CSO's website security without needing technical expertise. These steps help protect your website from attacks (e.g., defacement, DDoS) and ensure it remains a trusted platform for your mission:

1. Check if Your Website Uses HTTPS

- Visit your website and look for a padlock icon in the browser's address bar (before the URL) or "https://" at the start of the address.
- If you see "http://" or a "Not Secure" warning, contact your web host to enable HTTPS (e.g., ask for a free Let's Encrypt certificate).
- Example: Your site is "www.CSOexample.org". Ensure the address bar shows "https://www.CSOexample.org" with a padlock.
- If HTTPS is missing, email your web host: "Please enable HTTPS for our website."

2. Confirm Regular Backups

- Ask your web host or website manager if your website is backed up regularly (e.g., daily or weekly) and where backups are stored (e.g., cloud or external server).
- Request a test restore to ensure backups work (e.g., ask, "Can you restore our site to last week's version?").
- Example: Your website went offline after an attack. A recent backup lets you restore it quickly.
- Contact your host: "Do we have automatic website backups? How often are they done?"

3. Verify Website Software Updates

- Check with your web host or website manager if the Content Management System (CMS, e.g., WordPress, Joomla) and plugins/themes are updated regularly.
- Ask if updates are automatic or if someone checks them monthly.
- Example: An outdated WordPress plugin caused a CSO's site to be hacked. Regular updates prevent this.

• Email your host: “Are our CMS and plugins kept up-to-date? If not, please enable auto-updates.”

4. Secure Admin Access

• Ensure only trusted staff have website admin access. Check with your website manager to remove access for former staff or volunteers.

• Verify that admin accounts use strong passwords (e.g., 14+ characters, like “sunbird&glass7rain”) and two-factor authentication (2FA).

• Example: A former volunteer’s old login was used to deface a site. Removing unused accounts prevents this.

• Ask your website manager: “Who has admin access? Can we remove old accounts and enable 2FA?”

5. Check for Suspicious Website Changes

• Visit your website and look for unusual content (e.g., strange text, unfamiliar images, or redirects to other sites).

• Report any odd behavior to your web host or IT contact immediately.

• Example: a CSO’s homepage redirected to a scam site due to a hack. Early reporting fixed it quickly.

• Browse your site and note anything unusual. Contact your host: “Our site has [issue]; please investigate.”

6. Protect Against DDoS Attacks

• Ask your web host if they provide DDoS (Distributed Denial of Service) protection to keep your site online during traffic floods.

• Confirm if basic protections (e.g., Cloudflare’s free plan) are enabled.

• Example: A human rights CSO’s site went offline during a DDoS attack. Free DDoS protection kept it running.

• Email your host: “Do we have DDoS protection? Can we enable a free service like Cloudflare?”

7. Limit Public Access to Sensitive Pages

• Check if sensitive website pages (e.g., admin login, internal documents) are password-protected or hidden from public view.

- Ask your website manager to restrict access to only authorized users.
- Example: a CSO's donor list was accidentally made public. Password-protecting the page fixed the issue.
- Ask: "Are sensitive pages like admin logins protected? Can we add passwords if needed?"

8. Train Staff on Safe Website Use

- Remind staff and volunteers not to share admin credentials or post sensitive information (e.g., donor data) on the website.
- Share a quick tip: "Always log out of the website admin panel after use."
- Example: A staff member shared an admin password in an email, leading to a hack. Training prevents this.
- Send a team email: "Never share website login details. Log out after editing the site."

2.6 CHAPTER

6: COLLABORATION AND SUPPORT FOR DIGITAL SECURITY

Stronger Together: Collaboration and Support

Digital security is not solely an individual or organizational effort; it is a collective endeavor. Civil society organizations can greatly benefit from working together, sharing knowledge, and supporting each other in the face of cyberthreats. In this chapter, we discuss how collaboration can enhance security – from sharing information with peer CSOs and building a culture of security in the community, to educating the public and tapping into local and international support networks.

Sharing Information with Other CSOs

No CSO is an island, especially in the digital realm. Often, attacks or risks that target one organization may also affect others in the same sector or region. By sharing information about threats and best practices, CSOs can collectively improve their defenses.

Why Share? There may be hesitancy to share security incidents out of embarrassment or fear that it reveals vulnerability. However, the benefits usually outweigh the risks when done in the right setting. If your CSO fell victim to a phishing campaign, informing others can help them avoid that trap. It's similar to neighborhood watch: if one house is targeted by a scam, they warn the neighbors. In cybersecurity, this concept of **information sharing** is formalized in some sectors through ISACs (Information Sharing and Analysis Centers). While formal ISACs exist for industries like finance or health, CSOs can create their own informal sharing circles or groups.

What and How to Share:

- **Threat Alerts:** If you encounter a specific phishing email, malware file, or suspicious approach (like someone impersonating a donor), you can share indicators: e.g., "We received an email from address X with subject Y which was malicious. Be on the lookout." Provide enough detail for others to recognize it. Some CSO networks set up email lists or secure chat groups for such alerts.
- **Tactics and Lessons:** After experiencing an incident or even a drill, share what you learned, maybe anonymizing sensitive parts. For example, you could share: "We implemented two-factor auth on all our accounts, and it blocked multiple unauthorized login attempts. It's been worth the effort." This motivates others to adopt similar measures.
- **Policies and Training Materials:** Exchanging resources like sample security policies or training slide decks can be mutually beneficial. One CSO might have a great basic "Cybersecurity 101 for staff" presentation that they could distribute for others to adapt, rather than everyone reinventing the wheel.
- **Contacts for Help:** If you have a good experience with a security consultant or IT volunteer, you might share that contact with a fellow CSO in need (with permission, of course). Similarly, if a CSO member attends a cybersecurity workshop or webinar, they can pass key takeaways to peers who couldn't attend.
- **Joint Exercises:** Possibly organize joint events like a multi-organization security training or even a simulated phishing drill among a few CSOs. This not only improves skills but also fosters trust among participants.

Building Trust for Sharing: Security info is sensitive. To share candidly ("we got hacked by X method, lost Y data"), you need trust that peers won't misuse that info or judge harshly. Establish a norm of confidentiality. Perhaps form a small, trusted group first (like within a coalition or a working group of CSOs who know each other) before scaling wider. Some communities establish the Chatham House Rule (you can use the information, but not reveal who said it). Some may even sign a simple

memorandum on handling shared info carefully. Over time, as beneficial exchanges happen, trust grows.

Use of Platforms: Some platforms and tools can facilitate secure sharing:

- Encrypted email lists (using services or PGP if all participants can manage it, though PGP is tricky).
- Messaging groups on Signal or similar apps for quick heads-up on urgent issues.
- Possibly, use a platform like **Rocket. Chat** or **Matrix/Element** to create a closed forum for CSOs (self-hosted or on a reliable server) where they can discuss security topics away from the public eye.
- Some networks might partner with CERTs to feed them anonymized info and get advisories in return.

Successful Examples: There have been initiatives like the **"CyberPeace Cafe"** or CSO meetups on security. Also, **NetHope** (a consortium of humanitarian CSOs) works on shared cybersecurity guidelines and incident info, treating civil society infrastructure as critical. Another is the "Information Sharing and Analysis Organization (ISAO) for CSOs" concept that some have floated. In Europe, within EU projects (like perhaps the context of this curriculum), partner CSOs could set up a shared incident log or Slack channel specifically for this purpose.

By sharing timely information, CSOs can **transform an attack on one into an early warning for all**. It also makes efficient use of scarce expertise – one IT person in a lead CSO might effectively serve as an advisor to several partners through knowledge exchange.

Building a Community for Security

Beyond reactive information sharing, CSOs can proactively create a community culture that prioritizes digital security. A supportive community can pool resources, foster learning, and amplify advocacy for better security tools and policies.

Security Champions Network: Identify people within local civil society who have an interest or skills in cybersecurity. They could be tech-savvy staff, volunteers with IT backgrounds, or sympathetic academics. Form a

local "security champions" group that meets periodically (even virtually) to discuss issues and solutions. These champions can then act as point persons in their respective organizations. For example, maybe one CSO's IT officer teaches others how to harden their Wi-Fi networks, while another who learned about GDPR shares compliance tips.

Workshops and Training Events: Organize community training sessions, inviting multiple CSOs. Perhaps a quarterly workshop on topics like "Using Password Managers," "Securing Mobile Communications," or "How to Respond to a Cyberincident" – much of which comes from this book's content. By training together, CSO staff not only gain knowledge but also meet peers, which can form the trust basis for the info sharing we discussed. You can often get experts (from universities, companies, or government CERTs) to come give these workshops at low or no cost for nonprofits as part of CSR or community service. There's power in numbers – a corporate trainer might not do a free session for one CSO of five people, but for a collective audience of 50 from various CSOs, they might.

Peer Support and Mentoring: Encourage a buddy system: maybe pair a smaller CSO lacking IT support with a bigger CSO that has an IT department for some mentorship. For instance, a CSO that successfully implemented cloud security can mentor another just starting. This can be informal but provides quick help when needed ("Hey, how did you guys implement 2FA for all staff? Can you show us?").

Resource Pooling: Consider joint procurement or sharing of tools. A group of CSOs might get a bulk discount on security software or share a subscription (within license terms). Alternatively, if a CSO has a spare server or security appliance, maybe others can use the capacity on it. In some contexts, CSOs have set up shared IT services (like a common secure email server or a shared IT helpdesk across three or four organizations) to collectively afford higher-quality security than each could individually.

Community Advocacy: There is also a role for CSOs collectively to advocate for better cybersecurity conditions. For example, lobbying a donor community to fund cybersecurity capacity-building, or pushing software

providers to offer better nonprofit pricing or features (some non-profit coalitions have gotten Microsoft or Google to include free security add-ons for CSOs). Additionally, raising awareness with internet service providers or authorities about threats to civil society (like sophisticated phishing targeting activists) can lead to broader protective measures. Think of the concept "civil society as critical infrastructure" that NetHope described – by banding together, CSOs can make the case that they need protection akin to government or industry and thus attract support.

Solidarity in Incident Response: When a major incident happens (like a CSO is hit by a serious attack, or faces online harassment, etc.), a community stands stronger facing it. Other CSOs can assist with manpower, share the load of public messaging, or provide temporary services. There are instances, e.g., when one human rights group was DDoS attacked, others mirrored their website content to keep it available (like digital solidarity). Such cooperative defense shows adversaries that attacking one will rally many others, which can be a deterrent.

Sharing Success Stories: In building a positive community, share success tales as well (as will be highlighted in Chapter 7). If one CSO successfully fended off a phishing attempt thanks to training, celebrate that in the community newsletter. It motivates everyone that investing in security pays off. Recognize and thank those who help others with security (maybe at an annual CSO conference, give a shoutout to that one IT volunteer who travels around installing antivirus for free at different CSOs – that kind of morale boost fosters continued support).

By developing a tight-knit community around security, CSOs move from isolated, vulnerable targets to a resilient network. Attackers (whether criminals or oppressive regimes) often rely on picking off isolated organizations; a united front means information about their tactics spreads fast, and responses can be coordinated. As one maxim goes, "There is security in solidarity."

Informing the Public: Raising Digital Security Awareness

CSOs often serve as community educators and advocates. Digital security is not just an internal issue; many of the people you work with (beneficiaries, community members, activists, etc.) could also benefit from better security awareness. By extending digital security knowledge to your broader community, you multiply the impact and help create a safer civil society environment.

Community Workshops and Training: Consider hosting public workshops or webinars on basic digital security for your audience. For instance, if you're a youth organization, run a session on "Staying Safe on Social Media" for teens and their parents, covering privacy settings, cyberbullying, phishing, etc. If you work with human rights defenders, maybe a training on secure communication (using Signal, avoiding surveillance). These sessions can be integrated into your regular programming. Many CSOs already do training on related topics (e.g., media literacy, online privacy) – you can incorporate modules from this curriculum. Providing such education not only helps the community but also positions your CSO as a leader in addressing contemporary issues, which can strengthen your reputation and trust.

Develop Simple Educational Materials: You could create or adapt leaflets, infographics, or blog posts on security tips and share them publicly. For example, a one-pager titled "5 Ways to Protect Yourself Online" with easy steps (use strong passwords, don't click suspicious links, update software, etc.), which you distribute at events or on social media. Visual, non-technical language works best for public audiences. You might adapt content from national cybersecurity awareness campaigns (October Cybersecurity Month materials are often freely available in multiple languages via ENISA or others). Ensure materials are in the local language and contextually relevant (mention local scams people see, local support contacts). This also could tie into your organization's mission – e.g., a consumer rights CSO teaching about avoiding online fraud.

***Public Awareness Campaigns*:** If resources permit, run a campaign around digital security. This could be pegged to something like Safer Internet Day,

or some relevant local development (say, a spike in SMS scams in your area). Use your communication channels to regularly remind followers about security (tweet security tips, share news of current scams to watch out for, etc.). Some CSOs partner with telecom companies or media to broadcast security PSA messages. Even a small-scale campaign, like posting weekly "Security Tip Tuesday" on your Facebook page, can slowly raise awareness.

Leverage Media and Storytelling: People understand through stories. If appropriate, share anonymized stories of digital incidents and how they were overcome (perhaps as part of a blog or talk). For example, a story of how a community leader's email was hacked and used to send false messages, and what was learned from that. It can humanize the issue and alert others to be cautious. Media might also be interested if there's a trend (like increasing targeting of CSOs or activists online); an interview with your CSO on the topic can highlight the importance of digital security to a wider audience.

Lobby for Better Policies and Support: On a higher level, inform the public and policymakers about the needs of civil society in cybersecurity. CSOs can collectively advocate for government programs that assist CSOs with cybersecurity (some countries have grant programs or CERT special outreach). Also advocate for user-friendly security in technology products – e.g., pushing software companies to make secure settings the default so users are safer without needing extensive expertise. In the EU, for instance, there are dialogues on protecting civil society from cyberthreats; CSOs' voices in those forums ensure policy measures include them (like funding and training).

Collaborate with Schools and Libraries: Perhaps partner with local educational institutions or libraries to host joint sessions on digital literacy and security. Many public libraries hold computer classes; offering a security segment could be welcomed. Schools are increasingly needing to teach online safety; CSOs with expertise could support that curriculum. By helping educate youth and the general public, you're building a more security-conscious society, which indirectly protects your CSO too (fewer

compromised personal accounts that could lead to spear phishing of your organization, etc.).

Encourage Reporting and Dialogue: Urge the public you engage with to report cybercrime or suspicious incidents. Many individuals suffer silently or are too ashamed (as if someone fell for a scam). Create a climate where people can seek help – maybe your CSO can serve as a mediator to guide them to police or helplines if they're victims of online harassment or fraud. Some CSOs take on a role as digital rights advocates, highlighting issues like privacy or surveillance in society, which correlates with security awareness.

Align with Your Mission: Tailor public security education in line with your mission for coherence. For instance, if your CSO deals with women's rights and you know women activists face online harassment, focus awareness on that and how to handle it (block/report features, maintaining privacy). If you are an environmental CSO, you might highlight how false information spreads online and basic verification practices – a security adjacent topic (information integrity).

By informing the public, CSOs perform a two-fold service: protecting their constituents and reinforcing their own security by raising the overall security "hygiene" of the environment they operate in. It creates a virtuous cycle where an aware community is less likely to be a vector or victim of cyberincidents.

In summary, knowledge is power, and CSOs, as trusted community entities, are well-placed to disseminate that power widely.

Local and International Support Resources

In addition to peer collaboration and public awareness, there are formal support resources available to CSOs at local, regional, and international levels. Knowing what these are and how to access them can provide much-needed assistance, especially when facing sophisticated threats or needing resources beyond your capacity.

Local Resources:

• **National Cybersecurity Agencies/CERTs:** As mentioned earlier, many countries have a national CERT (Computer Emergency Response Team) or a cybersecurity agency that offers guidance. Some have programs focused on CSOs or small businesses. For example, the U.K.'s National Cyber Security Centre (NCSC) provides free guidance and even some free services (like web check, mail check) to improve security for organizations. Check if your country's CERT has an outreach or resources in your language (they often publish alert bulletins which you can follow).
• **Law Enforcement Cybercrime Units:** If you face issues like online fraud, harassment, or a targeted attack, local police cyberunits might help. Some countries have special units working with civil society (particularly in contexts of protecting journalists or activists). Build a relationship if possible – maybe invite an officer to speak at a CSO forum about reporting cyberincidents, so you demystify the process.
• **Academic Institutions:** Local universities, especially those with IT or cybersecurity departments, can be allies. Professors or students might take on CSO security as part of research or volunteer projects. For instance, a university IT club might do a security audit for your CSO as a class project (with your consent and under supervision). Some universities run cybersecurity clinics or have incubators for social tech solutions.
• **Tech Companies' Local Offices:** Big tech companies often have local presence and corporate social responsibility (CSR) programs. They sometimes run digital literacy or safety workshops (Google's online safety training, Meta's digital literacy campaign, etc.). Approach them to include your CSO staff or beneficiaries in those free trainings. They might also donate or discount security products. For example, Cisco has donated firewall hardware to some nonprofits through partnerships.
• **CSO Support Organizations:** Entities like tech federations or associations (e.g., TechSoup – a global CSO providing discounted software, including security suites; in Europe, perhaps the European

Network of Civil Society Security, etc., exists). TechSoup, specifically, offers not just software but also capacity-building resources and sometimes webinars on security. National CSO networks might also have working groups on ICT, where you can get advice.

International Resources:

- **Access Now's Digital Security Helpline:** Already mentioned, it's a globally available 24/7 rapid response team for civil society. They operate in multiple languages (24/7 in English, Spanish, French, and other languages). They can help with anything from malware removal guidance to mitigating DDoS to recovering accounts. It's free and confidential.
- **The CyberPeace Institute:** This organization not only analyzes cyberattacks on civil society but also coordinates assistance. Their CyberPeace Builders program has volunteers from tech companies offering pro-bono help to CSOs around the world. You may apply to be a beneficiary of their program, which could grant you recurring expertise, like help setting up secure infrastructure or policies.
- **International Freedom of Expression/Digital Rights Orgs:** Groups like Front Line Defenders, The Engine Room, EFF (Electronic Frontier Foundation), and others often publish guides or can connect you to experts. For instance, Front Line Defenders has a "Digital Protection" program and a Security in a Box toolkit tailor-made for human rights defenders (with tools and tactics).
- **Donor-Funded Programs:** There are sometimes donor-funded projects specifically to raise CSO cyber resilience. For example, in the EU, there have been projects under Erasmus+ or CEF focusing on enhancing digital skills, including security for nonprofits (like perhaps the KA220 project in your title is one). Keep an eye out for calls or networks under such projects; they often produce toolkits, host trainings, or offer consultation to participating CSOs.
- **Forums and Conferences:** Internationally, conferences like RightsCon, Internet Governance Forum (IGF), or regional cybersecurity conferences

sometimes have civil society tracks. Participating can connect you to a global community and resources. RightsCon in particular is all about digital rights and security for activists. Many sessions yield actionable advice or lead to funders who might support your security improvements.

- **Funding Opportunities:** International foundations have recognized cybersecurity as a critical capacity for civil society. For example, the Ford Foundation and Open Technology Fund have granted funds for CSO cybersecurity initiatives. The EU has funding lines under programs like Horizon or Digital Europe that might support capacity building if you partner or apply. If you need serious upgrades (like hiring an IT security staff or revamping IT infrastructure), consider integrating that into grant proposals for core support. Justify it as necessary risk mitigation – many donors are more aware now and might approve the budget for that.

Language and Cultural Relevance: When seeking help, try to find it in your language or context if possible. Global resources are great, but they may be in English or too general. This is why local experts and translating international guides into local languages is important. If, say, your CSO is in Türkiye (I see Istanbul timezone in prompt), using a local Turkish resource (like a Turkish CERT advisory or a digital security training in Turkish) might be more straightforward for staff. If you can't find some resource in your language, perhaps volunteer to translate a relevant guide – that itself is a community contribution.

Tech Donations: On support, note also things like Google for Nonprofits offers free G Suite, Microsoft for Nonprofits offers free O365 licenses, Okta offers free single sign-on solutions, and some security vendors have nonprofit donation programs (e.g., NortonLifeLock provides some CSO support). These can reduce cost barriers to using top-tier security tools.

Stay Updated: The threat landscape evolves. Make it a habit to follow some security news feeds or join mailing lists (some curated for CSOs). For example, the CIVICUS Cybersecurity mailing list (if it exists) or simply

following credible sources on social media (e.g., @enisa_eu on Twitter for EU news, or local cybersecurity firms' blogs).

In summary, you're not alone. There is a web of support from local to global. Proactively connecting with these resources during calm times (not just during a crisis) is worthwhile. Establish relationships with key contacts (know who you'd call at 10 p.m. if something went wrong). And equally, when you gain knowledge or resources, contribute back to these networks – that's what keeps them robust and available for the next CSO in need.

By leveraging collaboration (section 6.1, 6.2), educating the public (6.3), and reaching out to support systems (6.4), CSOs can transform digital security from a daunting solo battle into a community-supported effort. In the next chapter, we'll look at concrete examples and common pitfalls to further learn from real-world experience.

Chapter Summary

Chapter 6 provides frameworks for CSOs to proactively identify risks and prepare for cyberincidents. It guides organizations to assess critical assets (e.g., donor databases) and vulnerabilities, using simple risk assessment templates to prioritize threats like phishing or ransomware. The chapter outlines creating an incident response plan, detailing steps for detection, containment, communication, and recovery. For example, a CSO with a response plan can quickly restore data after a ransomware attack, minimizing damage. It emphasizes documenting incidents to learn from them and updating plans annually. The chapter addresses GDPR's 72-hour breach notification rule, ensuring compliance. Practical steps include assigning roles (e.g., a Data Protection Officer) and testing plans via tabletop exercises. The chapter's focus on preparation helps CSOs recover swiftly, reducing operational and reputational harm. By offering clear, low-cost frameworks, it empowers non-technical staff to contribute to resilience, aligning with the e-book's mission to make cybersecurity achievable for resource-constrained organizations.

Data Protection Policy Template for CSOs

Organization Name: [Insert CSO Name]

Effective Date: [Insert Date]

Last Updated: [Insert Date or "N/A for initial policy"]

This Data Protection Policy outlines how [CSO Name] collects, stores, accesses, and protects personal data to ensure privacy, security, and compliance with applicable laws (e.g., GDPR, [Insert Local Data Protection Law]). It applies to all staff, volunteers, and partners handling personal data, safeguarding the trust of our beneficiaries, donors, and stakeholders.

This policy covers all personal data (e.g., names, contact details, health, or financial information) managed by [CSO Name], including data related to beneficiaries, donors, staff, and volunteers.

1. Data Collection

We collect only the personal data necessary for our mission and programs, obtaining informed consent where required. Data is collected lawfully, transparently, and for specific purposes.

Procedures:

- Clearly explain why data is collected and how it will be used before collection (e.g., via consent forms or privacy notices).
- Collect minimal data to achieve the purpose (data minimization principle).
- Document the purpose of the collection and obtain consent where applicable (e.g., signed forms, online checkboxes).

2. Data Storage

We store personal data securely, using encryption and protected systems, to prevent unauthorized access, loss, or theft.

Procedures:

- Store data on secure platforms (e.g., encrypted cloud services like Google Drive with 2FA, or locked physical files).
- Encrypt sensitive data at rest (e.g., on laptops, external drives) and in transit (e.g., using HTTPS or secure email).

- Maintain regular backups (e.g., weekly to a secure cloud or external drive) to ensure data recovery.
- Dispose of data securely when no longer needed (e.g., shred paper records, use secure deletion tools for digital files).

3. Access Control

Access to personal data is restricted to authorized personnel who need it for their role, following the principle of least privilege.

Procedures:

- Assign access based on job roles (e.g., only program managers access beneficiary data).
- Use strong passwords and two-factor authentication (2FA) for all accounts with access to personal data.
- Regularly audit access permissions (e.g., monthly) to remove access for former staff or volunteers.
- Train staff and volunteers on secure data handling (e.g., not sharing passwords, logging out after use).

4. Breach Reporting

We promptly detect, respond to, and report data breaches to minimize harm and comply with legal obligations (e.g., GDPR's 72-hour notification rule).

Procedures:

- Designate a Data Protection Officer or point person (e.g., [Insert Name/Role]) to handle breaches.
- Report suspected breaches immediately to the designated person (e.g., via email to [Insert Email]).
- Notify the relevant data protection authority (e.g., [Insert Local Authority Name]) within 72 hours if a breach risks harming individuals.
- Inform affected individuals (e.g., beneficiaries, donors) if required, providing clear guidance on next steps.
- Document all breaches and responses to improve future prevention (e.g., update risk assessment).

5. Responsibilities

Leadership: Approve and fund the policy's implementation (e.g., budget for training, tools).

Staff and Volunteers: Follow this policy, report issues promptly, and attend data protection training.

Data Protection Officer/Point Person: Oversee policy compliance, manage breaches, and coordinate annual reviews.

6. Compliance and Review

Compliance: This policy aligns with GDPR and [Insert Local Data Protection Law]. Non-compliance may result in disciplinary action or legal penalties.

Review and update this policy annually or after significant changes (e.g., new programs, regulations). Next review: [Insert Date, e.g., November 2026].

All staff and volunteers receive data protection training at onboarding and annually.

7. Contact

For questions or to report a breach, contact: [Insert Data Protection Officer/Point Person Name, Email, Phone].

Local Data Protection Authority: [Insert Name and Contact Info, e.g., "Türkiye's Personal Data Protection Authority (KVKK), [contact details]".

Approved by: [Insert Leadership Name/Role, e.g., Executive Director]

Date: [Insert Date]

Customization Notes: Replace placeholders (e.g., [CSO Name], [Local Data Protection Law]) with your organization's details. Add local compliance requirements or specific tools as needed.

2.7 CHAPTER

7: SECURITY SUCCESSES IN CSOS

Real Stories: Security Successes in CSOs

It's encouraging to learn how peer organizations overcame security challenges. Here are a few anonymized but realistic scenarios showing positive outcomes thanks to good security practices:

Phishing Attempt Thwarted by Training: A human rights CSO in Eastern Europe received an email that looked like a Google Docs share from a colleague. Because staff had undergone phishing awareness training, one team member noticed something was off (the sender's email was slightly misspelled) and did not click the link. Instead, she alerted the IT focal point. They confirmed it was a credential-stealing phishing attempt. As a result, no account was compromised. This reinforced the value of training – the CSO's director highlighted in the next staff meeting how that employee's caution protected everyone, turning it into a teachable moment. It was a success in that an attack was prevented with zero damage, thanks to an alert staffer.

Ransomware Attack Survived Due to Backups: A mid-sized health CSO in Africa was hit by ransomware one morning – staff found their files encrypted and a ransom note on their screens. It was chaos initially. However, the organization had a robust backup system: all critical data was backed up to an external server nightly. Within hours, their IT consultant isolated the infected machines, wiped them, reinstalled software, and restored the data from the previous night's backup. They lost at most a day's work on a few documents. They did not pay the ransom and reported the incident. This experience turned into a security success story they share – their investment in backup and recovery planning paid off, proving how important it is. Later, they even presented this case in a webinar, encouraging other CSOs to implement offline backups.

Secure Communication Protected Sensitive Plans: An advocacy coalition was organizing a campaign in a country with heavy surveillance. They suspected their communications were being monitored. Under guidance from a digital security consultant, they switched to using end-to-end encrypted messaging (Signal) and email with PGP for the most sensitive attachments. During the campaign, they noticed attempts by adversaries to pre-empt their strategy, but critical details were never leaked. Post-campaign analysis suggested that since their switch to secure communications, the opposition lost its "inside knowledge" edge. The coalition credits the secure tools for safeguarding their plans and contributing to the campaign's success. It solidified their commitment to use encrypted channels for future operations and served as an example for others in their network.

Two-Factor Authentication Foiled Account Hijack: A women's rights CSO in South Asia had one of their staff's Gmail accounts targeted by a spear-phishing email. The staffer accidentally entered her password on a fake Google login page. That password went to the attacker. Shortly after, the attacker from another country tried logging into her Google account — but because the CSO had enforced two-factor authentication on all accounts, the login demanded a verification code from her phone. The attacker didn't have that, so he was stopped cold. Google alerted the user of a blocked sign-in attempt. She immediately realized what happened, reported it, and changed her password. In the end, 2FA turned what could have been a serious breach into a mere scare with no harm done. This real incident really drove home to the whole team why those somewhat annoying 2FA prompts were worth it. It was a day of relief and a victory for their security measures.

Community Collaboration Stopped DDoS: A network of environmental CSOs launched a campaign that drew the ire of some opponents, who then launched a Distributed Denial of Service (DDoS) attack on the network's joint website (flooding it with traffic to knock it offline). Individually, the CSOs had limited IT resources to mitigate this. However, through a tech solidarity channel, one CSO leader quickly reached out for help. A partner organization in a tech company arranged a temporary use of their DDoS

protection service (Cloudflare), and another CSO's IT staff helped reroute the site through that protection. Within a few hours, the website was back up despite facing an attack, and the campaign continued. This collaborative response was a success story illustrating how support from allies can counter even big cyberthreats. It also taught them to set up always-on Cloudflare protection thereafter. They later wrote this case in a blog to thank those who helped and to guide others on dealing with DDoS.

These stories demonstrate that even when CSOs are targeted by cyberthreats, **preparedness and quick action can lead to a successful defense or rapid recovery**. The common threads include: prior investment in security measures (training, backups, 2FA), quick recognition and response, and leveraging support networks. By sharing and studying such successes, CSOs can learn what really works and gain confidence that they, too, can handle similar situations.

Common Mistakes and How to Prevent Them

Learning from others' mistakes (or our own) is crucial in improving security. Here are some frequent pitfalls CSOs encounter, coupled with strategies to avoid them:

Using Weak or Default Passwords: Perhaps the most widespread mistake is sticking with easy passwords (like "123456", "password") or leaving default passwords unchanged on devices (e.g., routers often come with "admin/admin"). These are a gift to attackers. Prevention: Establish a password policy that requires strong, unique passwords and use password managers to handle them. During training, show examples of bad vs. good passwords. And whenever setting up new hardware/software, immediately change default credentials (and document them securely). Conduct occasional audits – use a tool or script to check if any accounts have weak passwords (some orgs use breach databases or auditing tools). Emphasize 2FA to compensate for any weak password that slips through.

Clicking Before Thinking (Phishing Success): Many breaches start with someone clicking a malicious link or attachment without scrutiny. The mistake is acting on an email or message impulse (especially ones invoking

urgency or curiosity) rather than verifying authenticity. Prevention: Training, training, training. Run simulated phishing tests to identify who needs more practice. Encourage a culture where it's okay to slow down and verify requests – e.g., "If an email seems urgent and asks for money or credentials, it's okay (in fact encouraged) to double-check with a call or separate 3email." Provide simple checklists: check sender address carefully, look for spelling errors, don't download unexpected attachments, etc. Additionally, technical defenses like good spam filters and link scanning help filter out the obvious fraud.

***Failing to Update Software Promptly*:** A common scenario: a CSO website runs on WordPress but hasn't updated plugins in a year, and an attacker exploits a known flaw to deface it. Or staff PCs still run older OS versions with unpatched vulnerabilities. The mistake is delaying or ignoring updates (sometimes out of fear it might break something, sometimes just forgetting). Prevention: Enable automatic updates wherever feasible. On systems that can't auto-update, assign someone the task to check monthly. Use tools that aggregate update needs (even simply turning on "Check for updates" notifications). For websites, consider managed hosting that handles the updates, or subscribe to plugin security mailing lists. Emphasize "patch Tuesday" or some routine. If resources allow, maintain an inventory of critical software and track their patch status (there are free scanners that highlight missing patches). Also, dispel myths like "updates slow down my computer" by showing the security risks of not updating.

Not Backing Up (or Testing Backups): Some organizations only realize the importance of backups after a data loss. Mistakes include not backing up at all, or having backups but not testing them (then finding they're incomplete or corrupted when needed). Prevention: Implement a 3-2-1 backup strategy (multiple copies, different media, one offsite). Schedule backups and automate them. More importantly, run test restores regularly. A simple drill: randomly pick a file and try restoring it from backup to ensure the process works. Also, ensure backups themselves are secured (encrypted and not accessible to the normal network, so ransomware can't hit them). Many have

learned the hard way that a backup on a network drive accessible to all is not safe from encryption malware. Solutions: offline backups or at least versioned cloud backups are immune to encryption.

Over-Privilege and Shared Accounts: Mistake: giving all users admin rights "because it's easier" or sharing one login among several people for convenience. This can lead to big issues – one person can inadvertently install malware with admin rights, or a departed employee still knows the shared account password. And accountability is lost when accounts are shared (you can't tell who did what). Prevention: Apply the least privilege principle. Create individual accounts for everyone, and give them only the access they need. Use role-based permissions for files and systems. Yes, it's a bit more initial setup, but modern systems make it fairly straightforward to manage users. Also, have a clear onboarding/offboarding checklist so access gets granted and revoked systematically. For admin tasks, have a separate admin account – do not browse the web or read email as an administrator user. That way, even if a user is tricked, the damage might be contained to their user level.

Ignoring Security Warnings or Best Practices: Humans sometimes ignore those browser warnings ("This site's certificate is not trusted") or disable security features because they seem annoying ("let me turn off the firewall to get this app working"). That can open doors to attack. Another example: using outdated, insecure protocols (like FTP instead of SFTP) out of habit. Prevention: Educate on why warnings exist. For instance, explain what a certificate warning means and that it could indicate a fake site or eavesdropping. Create an environment where if a security measure blocks something, instead of disabling it, staff ask for proper solutions (like add an exception if it's a known safe internal site, etc.). Provide guidance: if antivirus flags a file, don't just whitelist it out of frustration – contact IT to analyze if it's truly safe. Write simple internal FAQs: "If you see a security warning, do X." Also, when setting up new tools, do it securely from the start so staff won't be tempted to use insecure workarounds.

Lack of Incident Response Plan: Many CSOs are caught flat-footed during an incident – not knowing who to call or what steps to take, which wastes precious time. Mistake: no predefined incident plan or drills. Prevention: Develop a basic incident response plan (as done in Chapter 5) and ensure everyone knows the basics of it. It might just be a one-pager: "If something weird happens: disconnect from the internet, call this person, etc." Also, do at least a tabletop exercise: talk through a hypothetical "What if ransomware hit us, what would we do?" to spot gaps. Having a plan reduces mistakes during real crises, like turning the wrong system off or panicking.

By being aware of these common mistakes, a CSO can take proactive measures to avoid falling into those traps. It's often small changes in behavior or policy that make a big difference – like the habit of applying updates or double-checking before clicking. Encourage a philosophy that "**everyone is a stakeholder in security,"** so mistakes can be caught or prevented by collective diligence (e.g., peer review of suspicious emails – "Hey colleague, does this look legit to you?" can stop a mistake).

In sum: strengthen weak passwords, think before clicking, keep everything updated, backup diligently, limit privileges, heed warnings, and plan for the worst. Avoiding these common errors will dramatically improve your security stance with fairly little cost.

Test Your Own Security: Simple Exercises

It's one thing to read about security; it's another to put it into practice. Here are a few simple self-assessments and exercises you (and your team) can do to gauge and improve your security readiness. Think of them as "security drills" or check-ups:

Phishing Drill: Craft a harmless "fake phishing email" to test awareness within your team. For example, send an email from a non-organizational address but use your org name in the display, with a subject like "Urgent update required" and a link to a Google Form (that just says "Congrats, this was a test!"). See who clicks or submits info. The goal is educational, not gotcha: afterwards, reveal it and discuss clues that it was phishy (maybe slight address difference, urgent tone, etc.). If few fell for it, great – if some did, use it as a gentle training opportunity. Alternatively, use free tools like Google's phishing quiz or Phishing Simulation tools (some AV suites have this feature) in a controlled way.

Password Strength Check: Take a look at some passwords (without asking anyone to expose theirs, you can simulate common patterns). Use a password strength meter (many online, e.g., Passwordmeter.com) to test a sample of typical passwords versus recommended ones. Better, if using a password manager, see if it reports weak/reused passwords – many have a security audit feature. As an exercise, have everyone create a strong passphrase of four random words (e.g., "apple caravan tiger dance") and test its strength versus something like "Winter2020!" – the results often show the passphrase is stronger and easier to remember. This reinforces good password creation habits.

Backup Restore Drill: Test your backup. Simulate a scenario: "We lost file X, what do we do?" Actually, go to your backup location, retrieve the file, and open it to ensure it's intact. Or choose a date and pretend you must roll back everything to how it was then – can you retrieve that date's backup? Time how long does it take to restore a representative dataset. This not only verifies backups but also prepares you for real incidents by revealing if instructions/credentials for backups are readily available. Maybe assign

someone else (not the usual IT person) to try the restore using only documented steps to see if the process is clear enough.

Device Security Audit: Do a quick audit of your office computers and phones (with permission, of course). Check: Are all OS updated (open Windows Update or equivalent, see last update date)? Is the antivirus running and updated? Are firewalls on? Are any devices still using default passwords (e.g., log in to the office router and see if default creds work – if yes, big flag to change it)? See if screens auto-lock when idle. You can make a simple checklist and score each computer. Then fix any issues found and celebrate if most things were secure by default (it validates your config practices).

Email Spoof Test: An interesting exercise: show how easy it can be to spoof emails, to raise skepticism. Using a controlled environment (like a service that allows sending emails from a custom address you own, or even just modifying the "From" name in Gmail), send yourself an email that appears to be from, say, "" (but it came from another domain). Demonstrate to staff how, at first glance, it looks convincing, but the email headers or actual address show the truth. This exercise often shocks people, and thereafter, they check email addresses more carefully.

Permissions Cleanup: Take one shared folder or Google Drive and audit who has access. You might discover ex-volunteers still had access, or some files were public link-shared inadvertently. As a "mini exercise," revoke any unnecessary access and document it. It's like spring cleaning for access rights. This serves as a reminder to periodically do this.

Incident Role-play: Pick a scenario (like "laptop stolen from cafe" or "ransomware on server") and verbally walk through how you'd respond (who to call, what steps to take). Role-play with staff: one plays the panicked user, another the IT responder, etc. This low-key rehearsal can point out gaps ("Oh, we don't actually have the bank's number handy to call and freeze accounts if email was compromised," or "We realize we don't know the admin password to our website by memory if LastPass is inaccessible."). Better to find out now than during a real crisis.

Each exercise is meant to be simple and not time-consuming, but very insightful. Think of it like a fire drill for cyberthreats – you practice in a low-stakes setting so that in a real emergency, you know what to do and feel less anxious because you've done something similar before.

After each exercise, discuss results openly without blame. If something went wrong (e.g., half the team failed the phishing test), treat it as collective learning: maybe the phishing email was really sneaky – now everyone knows to be wary of that trick next time. If an exercise reveals a serious weakness, thank the process for uncovering it and commit to fixing it.

Regularly doing such exercises keeps security in people's minds and fosters a culture of continuous improvement. It demystifies security (because you're actively doing things, not just hearing policies). It can even be fun in a way – some organizations gamify it, offering small rewards to those who spot phishes or have the fewest issues in audits.

Integrating Digital Security into Daily Routine

The ultimate goal is for good security practices to become second nature – just a normal part of how you and your organization operate. Here are tips on weaving digital security seamlessly into everyday life at the CSO:

Start the Day with Security in Mind: Encourage simple morning habits. For example, when you boot up your computer, let it install updates first before diving into work (grab coffee while it updates rather than hitting "postpone"). Or check any security notifications (like "Windows Defender: no issues found" or a software update prompt) and address them early. This ensures you begin work in a secure state rather than ignoring those little shields and exclamation marks on your taskbar.

Password Manager Every Day: Make using the password manager a routine part of login processes. If set up properly, it can autofill credentials – so staff quickly see the benefit (faster login, no password reset hassles) and it just becomes how they log in. The daily routine shift is from "remember or writing down passwords" to "unlock manager once with a strong passphrase and then click to log in everywhere." Over time, they'll not imagine life without it. Some managers also prompt to update weak passwords – maybe

allocate a few minutes each Friday to update one flagged password. Bit by bit, all accounts get stronger passwords.

Team Reminders and Culture: Incorporate security tidbits into regular team meetings or internal newsletters. For instance, in a weekly meeting, one agenda item could be a one-minute security tip or news (e.g., "FYI, there's currently a WhatsApp scam going around; remember not to share verification codes"). This normalizes the conversation. It doesn't have to dominate, just a routine check-in. Some CSOs put up a "Security Tip of the Month" poster on the wall or Slack channel, which passively keeps awareness in daily sight.

Lock Screens and Clear Desks: Make it a habit to lock your computer (Win+L on Windows, Ctrl+Cmd+Q on Mac) whenever you step away – even for a minute. If everyone does it, it feels normal, not paranoid. Same with keeping sensitive papers or USB drives not lying around (the old "clear desk policy"). It's easier in routine if you tie it to something: e.g., at day's end, the last thing: back up files, lock all cabinets, check you logged out of systems – then you know you're set. Maybe create a printed checklist for closing up the office securely (digital and physical) that staff follow daily until it's second nature.

Integrate Security in Workflows: Whatever tools you use, use their security features by default. Example: if sharing a file via cloud, routinely use the "share with specific people" rather than the link. It takes maybe 10 seconds more to type their email, but if it becomes the only way people share, it's just normal. Or schedule periodic permission reviews as part of project closing: e.g., when a project finishes, part of the wrap-up checklist is "review and remove any external access from project folders." That way, security maintenance is baked into the project management life cycle.

Update Tuesday (or a chosen day): Many organizations schedule when they do maintenance tasks. Perhaps on Tuesday mornings, the IT/designated person ensures OS and apps are updated on all devices, or each user checks for phone updates weekly. If it's expected and scheduled, it won't be seen as an interruption but as routine (like watering the plants

every Monday, we update the systems). Cloud services update themselves, but maybe monthly check the admin console for any alerts or new security features to enable (providers add new security settings often; making time to integrate those regularly is good).

Continuous Learning: Encourage staff to take bite-sized online courses or quizzes occasionally. Maybe everyone does one module of an online security course per quarter (some are interactive and short). If you allocate, say, an hour of work time for it, it shows organizational commitment. This keeps knowledge fresh and signals that security is part of professional development, not an optional chore.

Lead by Example: Leadership should model security behaviors openly. If the director always uses a 2FA token and brags, "I love how secure and easy this is," others follow. If leadership falls for scams or uses weak practices, others will subconsciously think it's okay. So integrate it at the top – e.g., if a staff member sends sensitive data via personal email, a manager should gently correct it: "Please use our official account or encrypt that file – that's how we do things here." Over time, the group norms change.

Harness Automation: One way to have security without daily human effort is to automate. For instance, set all computers to auto-lock after five minutes of idle – then staff adapts to that pattern (and maybe finds five minutes too short, so they proactively lock when stepping out rather than being locked out mid-sentence). Use auto-updates, auto-scans (schedule AV full scans for lunch break time weekly). This reduces reliance on memory or motivation – the system supports the routine. Similarly, using a single sign-on (SSO) solution, if available, can integrate security (one strong login unlocks multiple apps, so users are always logging in with that one robust method rather than juggling weaker ones).

Reward and Reinforce: Positive reinforcement helps habits. Consider small rewards or recognition for good security behavior. Example: "Security Star of the Month" for someone who reported a phishing email or came up with an idea to improve security. Even just public praise, "Thanks to Alice for noticing the unusual email – great attention to detail!" encourages

everyone to be attentive. It shows that security mindfulness is appreciated, not just expected.

By embedding these practices into daily workflows, digital security stops being a sporadic project and becomes part of the organizational culture. New staff will absorb it from day one because "this is how we operate here." It demystifies security – it's not a special techie thing, it's part of everyone's routine job duties, much like locking the office door or wearing an ID badge. Over time, these small daily habits build a strong fortress almost invisibly. You might not even realize how secure you've become because it feels routine and easy. That's the goal: security not as a burden, but as an integrated aspect of working smarter and safer every day.

Chapter Summary

This chapter explores how CSOs can leverage collaboration and external resources to enhance digital security. It emphasizes that no organization faces cyberthreats alone, advocating for shared knowledge and networks. The chapter highlights free or community-driven tools, like Google Workspace for CSOs or digital security helplines, to address budget constraints. It encourages joining security forums and coalitions to share threat intelligence and success stories. Examples include CSOs partnering with tech volunteers to secure servers or accessing free resources from national CERTs. The chapter also promotes collaboration with government, academia, and tech industries to advocate for a safer digital ecosystem. By connecting with peers, CSOs amplify their defenses, as seen in a case where shared alerts stopped a phishing campaign. The chapter's practical guidance, like subscribing to security newsletters, ensures accessibility for small CSOs. It aligns with the curriculum's train-the-trainer model, fostering a community-driven approach to resilience and collective defense.

THREE:

EDUCATION MODULES

Introduction and Context

In today's digital age, civil society organizations (CSOs) and non-governmental organizations (NGOs) are increasingly reliant on digital tools to fulfill their missions. Unfortunately, this makes them attractive targets for cyberthreats. In fact, 50% of CSOs were targeted by a cyberattack in 2025, and nonprofits are now the second most targeted sector by nation-state cyberattacks (31% of all cases). Despite this risk, many CSOs are underprepared – four out of five CSOs lack any cybersecurity plan, and 70% do not feel they have the necessary knowledge or skills to respond to cyberattacks. These statistics underscore an urgent need to strengthen digital security capacity in the nonprofit sector.

Digital security is not just an IT issue; it impacts an organization's ability to serve its community. A single breach or ransomware attack can disrupt critical services, compromise sensitive beneficiary data, and damage public trust. For CSOs operating with limited resources, recovering from such incidents can divert precious funds and time away from their core mission. Enhancing the digital security infrastructure of civil society is therefore essential to ensure these organizations can operate safely and effectively.

Objective of the Curriculum

One key objective of our project is to develop a comprehensive "Digital Security Curriculum for Civil Society." The aim is to create a structured training program that will empower CSOs and civil society groups with the knowledge and skills needed to improve their digital security infrastructure. By infrastructure, we mean the whole spectrum of an organization's digital security posture – from secure technologies and practices to policies and staff capacities. This curriculum is envisioned as a practical toolkit to help CSOs learn how to protect their data, systems, and communications, thereby reducing their vulnerability to cyberthreats.

This objective aligns with our project's broader goal of increasing digital security across Europe. By building capacity at the civil society level, we take a bottom-up approach to bolster cybersecurity on a continental scale. Well-

trained CSOs will not only protect their own operations but also contribute to a more secure digital environment for the communities they serve. In essence, the curriculum will be a strategic step toward strengthening cybersecurity through civil society, ensuring that even smaller organizations can uphold strong digital defense practices.

By the end of this curriculum, participants will be able to:

- *Identify major digital security threats to CSOs and explain fundamental protective measures.*
- *Conduct a basic risk assessment of their organization's digital assets and draft a simple cybersecurity plan.*
- *Implement essential security measures on devices, networks, and communications (e.g., strong passwords, firewalls, secure Wi-Fi).*
- *Apply data protection principles and comply with relevant data privacy regulations (e.g., GDPR).*
- *Use secure social media and online tools to protect the organization's reputation and information.*
- *Develop and enforce basic IT security policies (such as password, backup, and acceptable-use policies) and execute a basic incident response procedure.*

Curriculum Overview

"The Digital Security Curriculum for Civil Society" is a structured learning program, designed as a strategic toolkit that civil society organizations and CSOs follow to strengthen their digital security infrastructure. The curriculum is delivered as a modular training package that project partners adapt and implement within their respective countries.

Key characteristics of the curriculum include:

- **Comprehensive Content:**

The curriculum covers topics from basic to advanced levels, enabling organizations with limited prior knowledge to progressively build their digital security capacity step-by-step.

- **Practical Focus:**

The curriculum emphasizes hands-on skills and real-life scenarios rather than theoretical approaches. Modules address practical situations such as responding to phishing attempts, securing online meetings, and protecting organizational data. Each module provides actionable guidance, tools, and checklists that CSOs apply directly in their daily operations.

- **Customization and Local Relevance:**

The curriculum is designed to be adaptable to national contexts. Project partners tailor examples, case studies, and selected content to local regulations, needs, and operational realities, while the core principles and learning objectives remain consistent across all partner countries.

- **Format and Delivery:**

Training materials include slide decks, concise explanatory texts, and interactive components such as exercises and quizzes. The curriculum is delivered through online formats and/or in-person workshops to ensure accessibility for organizations of different sizes and technical capacities. A train-the-trainer approach is promoted, enabling project partners and local experts to deliver the training in their national languages.

- **Outcome-oriented Structure:**

Upon completion of the curriculum, participants are able to assess their organization's digital risks, implement essential security measures, develop internal digital security policies, and respond confidently to common cyberthreats. The curriculum includes self-assessment tools and indicators that allow organizations to evaluate their level of digital security readiness.

Why CSOs Need Digital Security Capacity?

- ***High Risk, Low Resources***: CSOs often handle sensitive data (e.g., personal details of beneficiaries, donors) but operate on limited budgets that constrain their cybersecurity measures. Attackers know many CSOs are "cyberpoor but target-rich" – rich in data and funds, but poor in defenses.

- ***Growing Threat Landscape***: With increased digitalization (accelerated by the pandemic) and reliance on third-party online services, the attack surface for CSOs has grown. Phishing, malware, ransomware, and DDoS attacks against civil society are on the rise.
- ***Lack of Awareness and Training***: Many CSO staff and leaders have not had formal cybersecurity training. Some 90% of nonprofits do not regularly train staff in cyberhygiene. This gap leads to unsafe practices (like weak passwords or falling for phishing scams) that adversaries exploit.
- ***No Formal Policies***: Without guidance, few CSOs establish security policies or incident response plans – leaving them rudderless during an incident. Nearly 80% of CSOs have no cybersecurity policy/plan in place. A curriculum can help organizations create these internal policies and response strategies.
- ***Regulatory Pressure***: Data protection laws like the EU's General Data Protection Regulation (GDPR) – the world's most comprehensive data protection law – require organizations to protect personal data. CSOs must comply just as companies do, or risk legal and reputational consequences. Building knowledge of such regulations is a crucial part of digital security capacity.
- These challenges highlight why a dedicated curriculum is necessary. It will address the knowledge gap, promote a culture of security, and provide CSOs with a roadmap to develop their own cybersecurity plans, policies, and protections.

Target Audience and Stakeholders

The primary target group of the curriculum consists of civil society organizations (CSOs) and NGOs, including the following profiles:

- ***CSO Leadership and Management Staff:***

Individuals responsible for organizational strategy, risk management, and resource allocation, who require a clear understanding of digital security risks and institutional responsibilities.

• ***IT Staff or Technical Focal Points:***
Personnel responsible for implementing technical security measures and supporting secure digital practices within the organization.

• ***Programmatic and Operational Staff:***
Staff members who manage daily data flows, beneficiary information, financial records, and digital communication require a strong awareness of secure digital practices.

• ***Volunteers and Field Staff:***
Individuals who use organizational devices or handle sensitive information in field settings and need guidance on secure digital behavior.

• ***Partner Networks and Community Organizations:***
Organizations working in cooperation or coalitions with CSOs, ensuring that digital security practices extend across institutional networks.

Stakeholders involved in the development and implementation of the curriculum include project partner organizations from participating countries and cybersecurity and digital security experts. Input from specialized experts and institutions ensures that the curriculum aligns with internationally recognized best practices in digital security and data protection.

Key Modules and Topics in the Curriculum

The curriculum is organized into several modules, each focusing on a critical aspect of digital security. Below is an outline of key topics we plan to include:

1. Digital Security Fundamentals: Understanding the Threat Landscape and Basic Hygiene – Introduces why digital security matters for CSOs. Covers types of threats (malware, phishing, hacking, DDoS, etc.), threat actors (criminals, hostile governments targeting civil society), and fundamental best practices. Emphasis on creating a security mindset and basic habits (strong passwords, using two-factor authentication, regular software updates, avoiding suspicious emails).

2. Risk Assessment and Planning: Assessing Organizational Risks and Creating a Security Plan – Guides CSOs through identifying their digital assets and vulnerabilities. How to conduct a simple risk assessment (what do we have that others might attack? How might they do it? What are the consequences?). This module will lead organizations to draft or improve their cybersecurity plan (since currently 80% lack one) – including policies for data handling, access control, and an incident response procedure.

3. Securing Devices and Infrastructure: Protecting Computers, Networks, and Websites – Focuses on securing the technology a CSO uses. Topics include device security (antivirus, encryption of devices, secure device configuration), safe use of Wi-Fi and networks, using VPNs when appropriate, and securing websites (basics of web hosting security, backups, using HTTPS, protection against defacement or DDoS). Real examples of attacks (e.g., a case of website defacement that took a CSO offline for months) will illustrate the importance of these measures.

4. Secure Communication and Collaboration: Safe Email, Messaging, and Remote Work – Teaches how to communicate securely both internally and with external stakeholders. Covers email security (recognizing phishing, using encrypted email or secure email providers), messaging apps (choosing secure apps like Signal, enabling end-to-end encryption), and secure file sharing. Also addresses challenges of remote work: using secure connections, protecting video conferences, and managing accounts/credentials when working from home or on the move.

5. Data Protection and Privacy Compliance: Safeguarding Data & Understanding Legal Obligations – Emphasizes protecting sensitive data that CSOs collect (beneficiary data, donor info, etc.). Introduces principles of data protection: data minimization, encryption of data at rest and in transit, secure storage/backup, and proper data disposal. We will highlight relevant laws like GDPR – a leading data protection framework in Europe – and what compliance entails for CSOs (e.g., obtaining consent, securing personal data, reporting breaches). This module ensures organizations understand both ethical and legal responsibilities in handling data.

6. Social media and Online Presence Security: Protecting Organizational Reputation and Accounts – Many CSOs rely on social media for outreach. This topic covers securing social media accounts (strong passwords, two-factor auth, role-based access for multiple managers), guarding against account hijacking, and dealing with online harassment or misinformation campaigns. Also includes guidance on website content management, security, and safe online behavior that protects the CSO's reputation.

7. Developing a Security Culture: Staff Training, Policies, and Incident Response – Focuses on human factors and organizational measures. How to cultivate a culture where every staff member understands their role in cybersecurity. Guidance on writing simple IT security policies (acceptable use policy, bring-your-own-device rules, etc.), conducting regular staff awareness trainings (since oCSOing training is vital to keep 90% of staff from being the weak link), and establishing an incident response plan (steps to take if a breach happens, roles and responsibilities, communication strategy during a cybercrisis). We'll also cover basics of reporting incidents to authorities and learning from incidents

Implementation Strategy for the Curriculum

The development and deployment of this curriculum were carried out as a collaborative and phased process.

Curriculum Review and Localization:

Following the preparation of the initial draft, project partners reviewed the curriculum materials to ensure their relevance to local contexts. During this phase, partners proposed adaptations such as translating key terminology, incorporating country-specific case studies, and aligning recommendations with national legislation and common practices. As a result, the curriculum was structured with a core framework complemented by optional localized sections for each participating country.

Pilot Training:

The curriculum was piloted with a small group of CSO participants in selected partner countries. The pilot implementation was delivered either as

short module segments (approximately 15–20 minutes per module) or as a full-day workshop. Feedback collected during this phase focused on clarity, length, and practical usefulness of the content, and the curriculum was refined accordingly.

Train-the-Trainer Sessions:

To ensure scalability and sustainability, train-the-trainer sessions were organized for project partners and designated CSO representatives in each country. These sessions covered not only the curriculum content but also guided facilitation techniques, interactive exercises, and discussion prompts, enabling trainers to confidently deliver the material to wider audiences.

Rollout to CSOs (Capacity Building):

Following the train-the-trainer phase, partner organizations conducted national-level trainings for local CSOs and civil society actors. These trainings were delivered through webinars, in-person seminars, or integrated into existing capacity-building activities. Depending on local needs, trainings were structured as individual modules of 15–20 minutes or combined into longer workshops covering multiple modules.

Resources and OCSOing Support:

All curriculum materials and the accompanying handbook were compiled and shared in accessible formats, primarily as downloadable PDF resources. In addition, an online communication channel was established to allow participants and trainers to ask questions, exchange experiences, and share updates related to emerging threats or good security practices. This peer-learning environment supported continued engagement beyond the formal training sessions**.**

Monitoring and Evaluation:

Throughout the implementation process, monitoring and evaluation activities were conducted to assess the impact of the curriculum. Indicators included the number of CSOs trained, changes observed between pre- and post-training assessments, and qualitative feedback on organizational

improvements (such as the adoption of cybersecurity policies or new data-protection procedures). These findings were integrated into the project's overall monitoring framework to ensure that the curriculum effectively contributed to strengthening digital security practices among participating organizations.

By following this approach, the curriculum development and implementation process was inclusive and iterative, resulting in a final product that was well-adapted to the needs of civil society organizations across different national contexts.

3.1 MODULE

1: DIGITAL SECURITY FUNDAMENTALS – UNDERSTANDING THE THREAT LANDSCAPE AND BASIC HYGIENE

By the end of this module, the participant will be able to:

- *Explain why digital security is critical for CSOs and identify basic cyberhygiene practices.*
- *Recognize common cyberthreats (malware, phishing, DDoS, etc.) targeting civil society.*
- *Apply fundamental security habits (strong passwords, two-factor authentication, software updates, vigilance against suspicious emails).*

Learning Objectives:

- Raise awareness of why digital security is critical for CSOs and the specific cyberthreats targeting civil society.
- Identify common types of cyberattacks (e.g., malware, phishing, hacking, DDoS) and threat actors (criminal groups, hostile governments) that CSOs may face.
- Adopt fundamental cybersecurity best practices and habits (e.g., creating strong passwords, enabling two-factor authentication, keeping software updated, and recognizing suspicious communications).

Key Topics:

- The importance of digital security for CSOs – how cyberincidents can disrupt operations and compromise sensitive data.
- Overview of the threat landscape: common attack types like malware, phishing, hacking, DDoS, etc., and their rising incidence against civil society.

- Threat actors targeting CSOs: from cybercriminals seeking financial gain to hostile state-backed groups aiming to surveil or disrupt CSO activities.
- Basic cyberhygiene practices: using strong passwords and a password manager, enabling two-factor authentication, keeping software/antivirus up-to-date, and being cautious with suspicious emails or links.
- Building a security mindset among staff – encouraging vigilance and a culture where everyone takes responsibility for digital safety.

Sample Activities or Exercises:

- **Threat Brainstorming:** Participants list potential cyberthreats to their organization and discuss how each threat could impact their work.
- **Password Challenge:** Attendees evaluate the strength of sample passwords and learn how to create and manage strong passwords (e.g., passphrases, using a password manager).
- **Phishing Quiz:** Present example emails (some phishing, some legitimate) and have participants identify red flags that indicate a phishing attempt.
- **Case Study Discussion:** Describe a recent local cyberincident affecting CSOs – Analyze what happened in this incident and discuss which basic security measures might have prevented it.

Module 1 Case Study Example: Phishing Attack on a Community CSO

- **Context:** A small community CSO that provides food and aid to vulnerable populations relies on email and online donation platforms. The staff has had minimal cybersecurity training and relies on basic email security only.
- **Problem:** One morning, the CSO's finance officer received an urgent-sounding email from someone pretending to be a major donor. The email contained a suspicious link to update payment details. The officer clicked the link and entered login credentials for the CSO's bank account website, unaware it was a phishing site. Within hours, unauthorized withdrawals were made from the CSO's account, totaling thousands of

dollars. The CSO had to halt operations temporarily while recovering the funds and securing the accounts.

- **Outcome:** Following the incident, the CSO reviewed this security failure with the help of a tech-savvy volunteer. They implemented basic cyberhygiene measures immediately: enforcing strong, unique passwords and enabling two-factor authentication on all accounts. They also started regular staff training on recognizing phishing emails (looking for typos, checking sender addresses, etc.). In subsequent months, the CSO successfully avoided similar scams and restored trust with donors by being transparent about the improvements.

Discussion Questions:

» *What basic cybersecurity practice could have prevented the phishing attack in this case?*

» *Why did the staff member fall for the phishing email, and what steps could help staff recognize such scams in the future?*

» *How did the CSO recover from the incident, and what measures did they put in place to strengthen security afterward?*

Module 1 Assessment

- This module will be assessed with five short questions and one small task. A minimum score of 70% is required to pass.

Module 1 – Assessment: Short Questions

1. Why is digital security especially important for civil society organizations? (Briefly explain how cyberincidents can affect CSO operations or beneficiaries.) 2. Name two common cyberthreats that frequently target CSOs. (Example: phishing, malware, DDoS, etc.)
3. What is phishing, and how does it usually try to trick users? (Explain the basic method in one or two sentences.) 4. List two basic cyberhygiene practices that help prevent account compromise. (Example: strong passwords, two-factor authentication, regular updates.)
5. Mention one clear warning sign that an email might be a phishing attempt. (Example: urgent language, suspicious sender address,

unexpected links or attachments.) **Practical Task: Phishing Risk Identification**

Participants are given a short sample email (or scenario) related to CSO work (e.g., a donation update, funder message, or internal request).

Participants are asked to:

- Decide whether the message is legitimate or suspicious.
- Identify at least two warning signs (red flags) in the message.
- Write one concrete action they should take instead of clicking the link or responding directly (e.g., verify via another channel, report to a supervisor).

Assessment Criteria:

- Correctly identifies the email as suspicious or risky,
- Correctly points out at least two red flags,
- Suggests an appropriate safe response.

3.2 MODULE

2: RISK ASSESSMENT AND PLANNING – ASSESSING ORGANIZATIONAL RISKS AND CREATING A SECURITY PLAN

By the end of this module, the participant will be able to:

- *Identify the organization's critical digital assets and potential vulnerabilities.*
- *Conduct a basic risk assessment by estimating the likelihood and impact of threats to those assets.*
- *Draft a simple cybersecurity plan or policy covering data handling, access control, and an incident response outline.*

Learning Objectives:

- Understand how to identify an organization's critical digital assets (data, systems, accounts) and potential vulnerabilities.
- Conduct a basic risk assessment to evaluate threats to those assets and the potential impact on the organization.
- Develop or improve a cybersecurity plan/policy for the CSO, covering key areas such as data handling procedures, access controls, and incident response preparedness.

Key Topics:

- Identifying digital assets and data: mapping out what information and systems the CSO uses (e.g., donor databases, email accounts, websites) and why they might be targeted.
- Vulnerabilities and threats: understanding how to spot weaknesses (obsolete software, lack of backups, etc.) and imagining threat scenarios

(What might attackers target? How might they do it? What are the consequences?).

- Risk assessment process: evaluating the likelihood and impact of different threat scenarios, and prioritizing risks to address first.
- Creating a cybersecurity plan: drafting an organizational security policy that covers data protection practices, user access control, and an incident response procedure (especially important since ~80% of CSOs currently lack a formal security plan).
- Keeping the plan updated: assigning responsibility for periodically reviewing and updating the security plan as the organization grows or the threat landscape changes.

Sample Activities or Exercises:

- **Asset Inventory:** Participants list key digital assets (e.g., databases, email accounts, devices, cloud services) that their CSO relies on and identify what sensitive information is associated with each.
- **Risk Mapping:** For each listed asset, the group identifies possible threats or failure scenarios and rates their likelihood and impact (creating a simple risk matrix to visualize high-priority risks).
- **Plan Development:** Working in teams, participants draft a basic cybersecurity plan outline for a sample CSO. This should include sections on data handling policies, who has access to them, and steps to take if a security incident occurs. Teams then share their plans for feedback.
- **Local Risk Scenario:** (Case scenario examples are included in the country-specific localization sections.) Participants discuss this scenario and brainstorm how they would mitigate the risk, using elements of a security plan (policies, preventive measures, response steps).

Module 2 Case Study: Ignored Vulnerability Leads to Data Loss Context: A mid-sized CSO manages an internal server storing donor and beneficiary data. They know the server is important, but have no formal

documentation of its backups or risks. The staff assumed that the data was safe because "nothing bad has happened before."

Problem: A sudden power surge caused by a nearby storm damaged the CSO's server hardware, corrupting the data. Because the server hadn't been backed up in months, all donor records, project files, and financial data were lost. The CSO was forced to halt its programs for weeks. Donors had to resend information, and many records could not be recovered, leading to confusion and loss of trust.

Outcome: Realizing the severity of this failure, the CSO conducted a thorough risk assessment with outside help. They identified key assets (databases, website, email accounts) and threats (power loss, hardware failure, cyberattacks). They prioritized investing in an off-site backup system and setting up a regular backup schedule. The CSO drafted a basic cybersecurity plan, including procedures for data backups and recovery. Later, when minor system issues occurred, they successfully restored data from backups without interruption.

Discussion Questions:

- *What were the warning signs that the CSO was vulnerable before the disaster?*
- *Which elements should the CSO include in its new cybersecurity plan to prevent a similar loss?*
- *How did performing a risk assessment help the CSO improve its security and operations?*

Module 2 Assessment

This module will be assessed with five short questions and one small task. A minimum score of 70% is required to pass.

Module 2 – Assessment: Short Questions

- What is considered a digital asset in a CSO context? (Give two examples.)
- Why is it risky for an organization to rely on the assumption that "nothing bad has happened before"?

- What are the two main factors evaluated in a basic risk assessment? (Explain briefly.)
- Name two common vulnerabilities that can increase cybersecurity risks in CSOs.
- Why is it important to regularly review and update a cybersecurity plan?

Practical Task: Basic Risk Assessment Exercise Participants are asked to complete the following steps for a hypothetical or real CSO:

- List one critical digital asset (e.g., donor database, email system, website),
- Identify one possible threat to that asset (e.g., power outage, phishing attack, hardware failure), • Briefly describe one preventive measure that could reduce the risk (e.g., backups, access controls, two-factor authentication).

Assessment Criteria:

- The asset is clearly identified,
- The threat is realistic and relevant,
- The proposed preventive measure is appropriate.

3.3 MODULE

3: SECURING DEVICES AND INFRASTRUCTURE – PROTECTING COMPUTERS, NETWORKS, AND WEBSITES

By the end of this module, the participant will be able to:

- *Implement best practices to secure computers and mobile devices (installing updates, anti-malware, and encryption).*
- *Configure and protect organizational networks (secure Wi-Fi, use VPNs for remote access).*
- *Enhance website and server security (enable HTTPS, perform regular backups, and defend against common attacks like defacement or DDoS).*

Learning Objectives:

- Implement best practices for securing computers and mobile devices (e.g., installing anti-malware software, enabling device encryption, and configuring security settings properly).
- Protect organizational networks and internet access through safe Wi-Fi practices and use of secure connections (such as VPNs for remote access).
- Strengthen the security of the CSO's website and online infrastructure by using modern protection measures (HTTPS, backups, DDoS protection, etc.) and understanding how to respond to common attacks.

Key Topics:

- Device security essentials: installing and updating antivirus/anti-malware software on all computers, enabling firewalls, and using disk

encryption on laptops and smartphones to prevent data theft.

- Secure device configuration: enforcing strong device login passwords/PINs, removing or disabling unnecessary applications and services, and applying security patches or updates regularly.
- Network security basics: safe use of Wi-Fi (using trusted networks, securing office Wi-Fi with strong passwords and encryption), and when to use VPNs for encrypted connections (especially on public networks).
- Website and server security: maintaining updated website software (CMS, plugins), using HTTPS to encrypt web traffic, performing regular backups of site data, and implementing protections against common attacks like defacement or DDoS.
- Real-world examples of infrastructure attacks: for instance, a case of website defacement that took a CSO offline for months, underscoring the importance of proactive defenses.

Sample Activities or Exercises:

- **Device Security Audit:** Using a checklist, participants inspect a sample device (or their own, if appropriate) for basic security protections – checking for antivirus installation and updates, firewall status, encryption enabled, and recent security updates.
- **Wi-Fi Safety Demo:** The trainer demonstrates the risks of using unsecured public Wi-Fi (e.g., how easy it is to snoop on traffic). Then discuss steps to stay safe: configuring a secure home/office Wi-Fi network and using VPN or secure apps when on public networks.
- **Website Security Review:** Present a fictitious CSO website scenario with several security flaws (outdated software, no HTTPS, weak admin password). Small groups identify the issues and recommend fixes to improve the website's security.
- **Local Case Study:** Describe a local case of CSO website defacement or cyberattack – Discuss what happened in this incident and what preventative measures (from the module's key topics) could help avoid such an event in the future.

Module 3 Case Study: Website Defacement and Service Outage
Context: A CSO runs a public website for program updates and fundraising. The site is built on an open-source content management system (CMS). The technical maintenance was handled by a single volunteer who occasionally updated the site.

Problem: Hackers exploited an outdated plugin on the CSO's website, defacing the homepage and replacing it with a political message. The CSO did not notice the change immediately because the staff was not checking the site regularly. The defacement remained for several days, causing confusion among supporters and temporarily dissuading donors. Visitors saw inappropriate content, and the organization's credibility was damaged. Additionally, the hackers gained access to the website's files, raising concerns about the security of donor data (though no breach was confirmed).

Outcome: After discovering the issue, the CSO took the website offline for clean-up and removed the malicious content. They updated the CMS and all plugins to the latest versions. Going forward, the CSO implemented regular site backups and scheduled weekly checks of its website. They also transitioned to a managed hosting provider with automatic updates and HTTPS encryption. In the following months, the site remained secure, and the CSO regained trust by communicating transparently about the incident and the steps taken to prevent it.

Discussion Questions:

» *How could keeping software up-to-date and regular backups have changed the outcome of this attack?*

» *What immediate steps should the CSO have taken once they noticed the website defacement?*

» *What long-term measures did the CSO implement to secure its web infrastructure?*

Module 3 Assessment

This module will be assessed with five short questions and one small task. A minimum score of 70% is required to pass.

Module 3 – Assessment

Short Questions

1. Why is device encryption important for laptops and smartphones used by CSOs?

(Answer in one or two sentences.)

2. Name two basic security measures that should be enabled on all organizational devices.

3. What are the main risks of using unsecured public Wi-Fi without additional protection?

4. Why are outdated CMS plugins a serious security risk for CSO websites?

5. How do regular backups reduce the impact of website defacement or cyberattacks?

Practical Task: Basic Device or Website Security Check Participants choose one of the following options:

Option A – Device Security

- List **three security measures** currently applied to one work device (computer or smartphone) *(e.g., antivirus, encryption, screen lock, updates)*
- Identify **one missing or weak measure** and briefly state how it could be improved.

Option B – Website Security

- Identify **two basic security controls** that should be in place for a CSO website.

(e.g., HTTPS, regular updates, backups, strong admin passwords) • Briefly explain **one risk** if these controls are not implemented.

Assessment Criteria:

- Measures identified are relevant to the module.
- Risks or improvements are realistic and clearly explained.

Passing Requirement:

The participant must correctly identify at least two valid security measures and one associated risk or improvement.

3.4 MODULE

4: SECURE COMMUNICATION AND COLLABORATION – SAFE EMAIL, MESSAGING, AND REMOTE WORK

By the end of this module, the participant will be able to:

- *Recognize and avoid common email-based threats (such as phishing) and apply secure email practices (strong passwords, 2FA).*
- *Use secure messaging and file-sharing tools that provide encryption.*
- *Implement safe remote work practices (using VPNs on public networks, securing virtual meetings with passwords).*

Learning Objectives:

- Recognize and avoid common email-based threats (such as phishing scams) and apply secure email practices in day-to-day work.
- Choose and use secure communication tools for messaging and file sharing (e.g., end-to-end encrypted apps, secure document collaboration platforms) to protect sensitive information.
- Implement security measures for remote work and virtual collaboration (using secure networks, protecting online meetings, and managing accounts/devices when working off-site).

Key Topics:

- **Email security:** How to spot phishing attempts (e.g., suspicious senders or links, urgent, unusual requests) and the importance of using strong passwords and 2FA for email accounts. If sensitive data is exchanged, consider encrypted email services or add-ons.
- **Secure messaging:** Selecting trusted messaging applications that offer end-to-end encryption (for example, Signal or other secure messengers)

and enabling security features like disappearing messages. Guidance on verifying contacts and not sharing sensitive info over insecure channels.

- **File sharing and collaboration:** Using secure cloud storage or file-sharing services that offer encryption. Practices like password-protecting sensitive documents or using platforms designed for secure collaboration when working with external partners.
- **Remote work safeguards:** Best practices for working outside the office, including using VPNs on untrusted networks, securing home Wi-Fi routers, protecting virtual meeting spaces (using waiting rooms, meeting passwords, limiting screen sharing), and managing work devices that are used remotely.
- **Balancing security and accessibility:** Ensuring that security measures (like encryption and access controls) are user-friendly enough that staff will consistently use them, and providing training on any new communication tool introduced for security reasons.

Sample Activities or Exercises:

- **Phishing Email Drill:** The facilitator shares sample emails with the group. Participants must decide for each whether it's a legitimate email or a phishing attempt, and highlight the clues that informed their decision.
- **Messaging App Comparison:** Break into small groups; each group reviews a different messaging app (e.g., WhatsApp, Signal, Telegram) and reports on its security features (encryption, two-factor authentication, etc.) and any limitations. Discuss which apps are most appropriate for various types of CSO communications.
- **Secure Video Call Setup:** Live demonstration of setting up an online meeting with proper security: enabling the waiting room, requiring a meeting passcode, restricting participant screen sharing, etc. After the demo, participants practice configuring these settings or discuss experiences securing their own meetings.
- **Local Context Discussion:** [Insert a secure communication tool popular in your country or a relevant encryption law] – Discuss how this

local context affects the CSO's communication security. For example, if a particular encrypted app is widely used locally, how can the CSO leverage it? If there are local regulations on encryption or data storage, how do they impact communication choices?

Module 4 Case Study: Remote Work Email Breach Context: During a humanitarian crisis, a CSO's field officer works remotely from a café using public Wi-Fi to send situation reports to headquarters. The organization uses email for daily communications, but does not enforce encrypted connections for remote users.

Problem: A cybercriminal on the same public Wi-Fi network intercepted the officer's unencrypted email traffic. The attacker obtained login credentials when the officer logged into the CSO's email account. Over the next day, the attacker impersonated the officer, sending fraudulent emails to donors requesting emergency funds for a fake project. One donor wired money to the attacker's account before the scam was detected. The CSO lost funds and had to explain the deception to donors.

Outcome: In response, the CSO implemented secure communication practices. All staff working remotely were required to use a VPN or HTTPS for email access, and two-factor authentication was enabled on email accounts. The CSO also adopted an encrypted messaging app for internal communications. They communicated with donors about verifying any future requests and improved email training for staff (spotting email fakes, not using public Wi-Fi without protection). No further incidents occurred after these measures.

Discussion Questions:

- *What vulnerabilities did the CSO's remote work practices have in this case?*
- *How could VPNs and two-factor authentication have prevented the attacker from gaining access?*
- *What steps did the CSO take after the breach to protect communications and donor trust?*

Module 4 Assessment

This module will be assessed with five short questions and one small task. A minimum score of 70% is required to pass.

Module 4 – Assessment 5 Short Questions

1. What are two common signs that an email might be a phishing attempt?
(Answer briefly.)
2. Why is two-factor authentication (2FA) especially important for email accounts used by CSOs?
3. Name one secure messaging feature that helps protect sensitive communications.
4. What risks do CSOs face when staff work remotely using public Wi-Fi without protection?
5. How can securing online meetings (e.g., passwords, waiting rooms) reduce security risks?

Practical Task: Secure Communication Check Participants complete the following task individually or in pairs:

1. Choose one communication channel used by your CSO
(email, messaging app, file-sharing platform, or video meeting tool).
2. Briefly answer:
» **One security measure is currently in place**
(e.g., 2FA enabled, encrypted messaging, meeting passwords) » **One improvement** that could strengthen security *(e.g., enabling VPN use, switching to an encrypted app, limiting access rights)* 3. Explain in **one or two sentences** how this improvement would reduce risk.

Assessment Criteria:

- The chosen channel is relevant to CSO communication,
- The security measures and improvements are realistic,
- The explanation shows understanding of secure communication practices.

3.5 MODULE

5: DATA PROTECTION AND PRIVACY COMPLIANCE – SAFEGUARDING DATA & UNDERSTANDING LEGAL OBLIGATIONS

By the end of this module, the participant will be able to:

- *Identify the sensitive data the CSO collects and explain why it must be protected.*
- *Apply key data protection practices (data minimization, encryption, secure storage, regular backups, and safe disposal).*
- *Understand and outline the CSO's legal obligations under data protection laws (such as GDPR) and how to ensure compliance.*

Learning Objectives:

- Recognize the types of sensitive data (e.g., beneficiary personal information, donor records) that CSOs collect and why it is crucial to safeguard such data.
- Apply key data protection principles – including data minimization, encryption (for data at rest and in transit), secure storage/backup, and proper disposal of data – to enhance privacy and security.
- Understand legal obligations and frameworks for data protection, such as the EU's GDPR and equivalent national data protection laws, and how to ensure the CSO complies with these regulations.

Key Topics:

- **Identifying sensitive data:** What counts as personal or sensitive data in a CSO context (names, addresses, health or legal case information, etc.),

and the risks if such data is leaked.

- **Data protection principles:** Practical steps for data minimization (only collecting what is truly needed), encrypting data at rest (e.g., files on drives) and in transit (using SSL/HTTPS for data transfer), secure data storage solutions (physical and cloud), maintaining regular backups, and properly deleting data that's no longer needed.
- **Legal frameworks:** Overview of major data protection laws – for example, GDPR (General Data Protection Regulation) as a leading framework in Europe, and [Insert your country's data protection regulation here]. Key obligations include obtaining informed consent for data collection, securing personal data through technical and organizational measures, and breach notification requirements.
- **Ethical data handling:** Beyond legal rules, emphasizing the ethical responsibility to protect individuals' privacy. Discussion of consequences of data breaches for CSOs, including harm to beneficiaries, loss of trust, legal penalties, and reputational damage.
- **Building compliance into practice:** How CSOs can develop simple privacy policies, data handling guidelines, and train staff on these policies. Introduction to concepts like Data Protection Officers (if relevant) or data handling agreements when working with partners.

Sample Activities or Exercises:

- **Data Audit Exercise:** Participants enumerate the kinds of personal data their CSO collects or handles and map out where that data is stored (databases, spreadsheets, email, cloud services). They then discuss for each item: who has access, how it's protected currently, and any gaps they notice.
- **Encryption Demo:** The trainer demonstrates encrypting a sample file or folder (or using an encryption tool for emails/text). Participants learn how encrypted data looks and practice encrypting and decrypting a piece of test data, emphasizing the importance of key/password management.

- **Policy Review:** Provide a template or example of a simple Data Protection Policy or Privacy Notice. In small groups, participants identify how this document addresses GDPR requirements and consider what changes would be needed to comply with [Insert your country's data protection regulation here]. Each group can present one key point they'd include in their own CSO's policy.
- **Legal Compliance Discussion:** Review a checklist of actions for GDPR compliance (e.g., appointing a responsible person, having consent forms, data breach plan). Participants discuss which items on the list they have in place and which they need to implement. Emphasize any additional steps required by national law (e.g., registering with a data protection authority if required by [Insert your country's data protection regulation here]).

Module 5 Case Study: Donor Database Breach

Context: An international aid CSO maintains a database of donor information (names, contact details, donation history) and beneficiary data (sensitive health information). The data is stored on an internal network drive accessible to program staff.

Problem: During a system upgrade, an administrator accidentally exposed the donor database folder on a public cloud file-sharing link without encryption or access controls. A hacker discovered the link and downloaded the entire donor list. Personal information of thousands of donors (names, emails, and donation amounts) was leaked online. The CSO was forced to notify donors of the breach as required by law. Several donors withdrew support, citing loss of trust. The CSO also faced scrutiny for not securing the data properly.

Outcome: After the breach, the CSO revised its data handling practices. They encrypted all sensitive data at rest and in transit, and restricted access to the database by implementing strong access controls. They also applied data minimization by removing unnecessary personal details from public files. The CSO appointed a data protection officer to oversee compliance and drafted a clear privacy policy. Training was given to staff on proper data

handling, and future sharing was done with secure links and passwords. The CSO regained confidence from its donors by quickly tightening security and transparently reporting the improvements.

Discussion Questions:

- *What data protection failures led to this breach, and how could they have been prevented?*
- *Which data protection practices (from this module's topics) did the CSO adopt after the incident?*
- *What legal obligations did the CSO have to address this breach, and why is compliance important for CSOs?*

Module 5 Assessment

This module will be assessed with five short questions and one small task. A minimum score of 70% is required to pass.

Module 5 - Assessment

Short Questions

1. What types of personal or sensitive data do CSOs commonly collect, and why must this data be protected?
2. Explain the principle of data minimization and give one practical example of how a CSO can apply it.
3. What is the difference between encrypting data at rest and encrypting data in transit?
4. Under GDPR (or equivalent national data protection laws), what is a CSO required to do in the event of a personal data breach?
5. Why is ethical data handling important for CSOs beyond legal compliance? Mention one potential consequence of failing to protect data properly.

Practical Task: Mini Data Protection Review

Participants are asked to complete the following task:

- Identify **one type of personal or sensitive data** collected by their CSO (e.g., beneficiary records, donor contact details, staff information).

- Briefly describe:
  » Where this data is stored (e.g., computer, cloud service, email, paper files),
  » Who has access to it,
  » One improvement that could be made to better protect this data (e.g., encryption, restricted access, data minimization).

Participants should present their answers **in three to five short bullet points** or discuss them briefly in small groups.

FOUR:

COUNTRY-BASED LEGAL AND REGULATORY FRAMEWORKS

390 313
49 9 7 9 2 9 7 3 43 443 3 5 3

3.6 MODULE

6: SOCIAL MEDIA AND ONLINE PRESENCE SECURITY – PROTECTING ORGANIZATIONAL REPUTATION AND ACCOUNTS

By the end of this module, the participant will be able to:

- *Apply security measures to protect the CSO's social media accounts (strong, unique passwords, two-factor authentication, limited admin roles).*
- *Respond effectively to social media incidents (account hijacking or impersonation) by following reporting and communication procedures.*
- *Implement best practices for maintaining a secure online presence (regular updates to the website/CMS, staff guidelines for posting and responding to misinformation).*

Learning Objectives:

- Implement security measures to protect the CSO's social media accounts (strong authentication, monitored access, regular audits of account settings).
- Develop strategies to safeguard the organization's online presence and reputation, including how to respond to account hijacking, impersonation, or misinformation attacks.
- Apply best practices for website content management and staff conduct online to ensure consistent and secure organizational representation on the internet.

Key Topics:

- **Social media account security:** Ensuring all organizational social media accounts use strong, unique passwords and have two-factor authentication enabled. Managing multiple administrators safely (using role-based access controls or team collaboration features, rather than sharing passwords).
- **Account monitoring and recovery:** Keeping an eye on account activity (so any unauthorized access is caught early) and knowing how to recover accounts if they are compromised (understanding platform support processes for hacked accounts).
- **Handling hijacking and impersonation:** Steps to take if a CSO's account is hijacked or if fake accounts impersonate the CSO – including reporting mechanisms on social platforms, communicating with supporters to clarify misinformation, and regaining control of accounts.
- **Dealing with online harassment and misinformation:** Tactics for responding to trolls or coordinated harassment campaigns (e.g., documenting abuse, using block/report functions, having a moderation policy for comments). How to counter misinformation or defamation online with factual messaging without amplifying false claims.
- **Website and content management security:** Keeping the CSO's website secure and reputable – updating the website CMS/plugins regularly, using secure passwords for site admins, limiting who can publish content, and having a process to quickly correct or take down incorrect or unauthorized content.
- **Reputation management:** Training staff and volunteers on guidelines for representing the organization online (personal social media use policies, what not to post about work, how to respond if they see misinformation), to maintain a positive and secure online presence for the CSO.

Sample Activities or Exercises:

- **Account Security Check:** Participants conduct a quick audit of one of the CSO's social media accounts. They verify if 2FA is enabled, passwords are strong/recently updated, recovery contact info is correct,

and only authorized people have access. They then create a to-do list for any improvements needed.

- **Incident Role-Play:** Simulate a scenario where a CSO's official social media account has been hijacked or a fake account is spreading false information about the organization. The team must decide on an immediate action plan: who will communicate to the public, how to alert the platform and followers, and what steps to secure or recover the account. After the role-play, discuss what went well and what could be improved in their response.
- **Harassment Response Plan:** In groups, participants draft a simple protocol for handling online harassment or hate campaigns. This might include steps like: do not engage publicly in anger, document the offending posts, report them to the platform, alert the CSO's management, and support any staff targeted. Groups share their plans and discuss common elements.
- **Local Example Discussion:** [Describe a recent local social media-related incident involving a CSO] – Analyze what occurred and how having robust social media security practices and an incident response plan could help manage or prevent such a situation.

Module 6 Case Study: Social Media Account Hijacking

Context: An environmental CSO uses social media (Twitter and Facebook) to engage donors and share campaign news. Multiple staff members have access to the accounts with shared passwords, and no one monitors login activity closely.

Problem: One morning, the CSO's Twitter account began posting inflammatory political messages unrelated to the CSO's mission. Followers were confused, and some accused the CSO of taking a political stance. The posts were the work of a hacker who had gained access after one staff member reused a common password. By the time the staff realized the breach, the messages had been retweeted by supporters, causing reputational damage. It took hours to regain access through the platform's support process, during which time negative impressions spread online.

Outcome: The CSO conducted an incident response by immediately posting a clarification on all channels, apologizing for the breach. They reset all social media passwords and enabled two-factor authentication on all accounts. They also set up role-based access (assigning specific admin accounts rather than sharing passwords). The staff reviewed and updated the website content to ensure no outdated information remained. The CSO established a policy for monitoring account activity daily. As a result, they were able to restore normal communications and later even gained support for being transparent. The new security measures prevented further hijacking attempts.

Discussion Questions:

- *What were the key failures that allowed the account hijacking to happen?*
- *How did the CSO respond to mitigate the damage, both technologically and in communications?*
- *Which security improvements did the CSO implement to protect its social media presence going forward?*

Module 6 Assessment

This module will be assessed with five short questions and one small task. A minimum score of 70% is required to pass.

Module 6 - Assessment

Short Questions

1. Why is it important for CSOs to use strong, unique passwords and two-factor authentication on social media accounts?
2. What risks can arise from sharing social media account passwords among multiple staff members?
3. What immediate steps should a CSO take if its social media account is hijacked or compromised?
4. How can online misinformation or impersonation affect a CSO's reputation and public trust?
5. Why is it important to have clear staff guidelines for online behavior and representation of the organization?

Practical Task: Social Media Security Review

Participants are asked to complete the following task:

- Choose one official social media account of their CSO (or a hypothetical CSO).
- Briefly describe:
  - » Whether two-factor authentication is enabled,
  - » How access is currently managed (shared passwords vs. role-based access),
  - » One concrete action that could improve the security or monitoring of this account.

Participants should summarize their answers in three-five short bullet points or discuss them briefly in small groups.

3.7 MODULE

7: DEVELOPING A SECURITY CULTURE – STAFF TRAINING, POLICIES, AND INCIDENT RESPONSE

By the end of this module, the participant will be able to:

- *Foster a security-conscious culture in the organization by engaging leadership and staff.*
- *Develop basic IT security policies (e.g., acceptable use, BYOD, password rules) and plan regular security training for all staff.*
- *Create and rehearse a simple incident response plan (defining roles, steps, and communication) to handle cyberincidents efficiently.*

Learning Objectives:

- Foster a security-conscious culture within the CSO, where every staff member understands their personal role in maintaining cybersecurity.
- Develop basic IT security policies (e.g., acceptable use of technology, bring-your-own-device rules) and implement regular staff training programs to reinforce good security practices.
- Establish and rehearse an incident response plan so the organization can respond effectively to cybersecurity incidents (clearly defining steps, roles, and communication channels).

Key Topics:

- **Building a cybersecurity culture:** How to get leadership buy-in and staff engagement for security initiatives. Creating an environment where employees feel responsible for protecting data and systems, rather than seeing security as solely the IT person's job.

- **Basic security policies:** Drafting simple, clear policies that set expectations for safe use of technology. Examples include an Acceptable Use Policy (what is allowed/prohibited on work devices and accounts), BYOD (bring-your-own-device) guidelines if staff use personal devices for work, and rules for creating and managing passwords.
- **Continuous staff awareness and training:** The importance of oCSOing education (workshops, newsletters, phishing simulation tests) to keep security knowledge fresh. Noting that regular training is vital since untrained staff can become the weakest link in security.
- **Incident response planning:** Key components of an incident response plan – how to detect and report an incident, immediate steps to contain the issue (e.g., disconnecting affected computers), roles and responsibilities (who leads the response, who communicates with stakeholders), and how to keep operations running during disruptions.
- **Reporting and learning from incidents:** Guidelines on when and how to report cyberincidents to authorities or regulators (especially if personal data is involved), and conducting a post-incident review to improve future resilience.

Sample Activities or Exercises:

- **Policy Writing Workshop:** Participants create a draft for one short security policy relevant to their CSO (for example, an Acceptable Use Policy for office computers, or a Mobile Device Policy). Each group writes a few key rules and then shares with everyone, inviting feedback to ensure the policies are clear and actionable.
- **Security Awareness Drill:** Organize a mock phishing exercise or a surprise "USB drop" (leaving a USB thumb drive as if it were found, to see if anyone plugs it in). Afterwards, discuss the results: how did the staff react? What were the red flags? Use this as a learning opportunity to reinforce training points in a safe environment.
- **Incident Response Tabletop:** Present a hypothetical cybersecurity incident (e.g., a ransomware attack encrypting CSO data). Have the team walk through their response step-by-step: how do they identify the scope

of the problem, who do they call first, how do they communicate to staff and possibly the public, and how do they recover systems or data? After the exercise, debrief on what went well and what roles or steps need clarification in their plan.

- **Local Reporting Info:** [Insert your country's cyberincident reporting mechanism or relevant authority contact here] – Make sure participants are aware of how to report a serious cybersecurity incident in their local context (for instance, notifying a national CERT or law enforcement), and discuss any legal requirements for breach reporting that apply to CSOs in their country.

Module 7 Case Study: Unsecured USB Leading to Malware Outbreak

Context: A CSO office allowed staff to use personal USB drives on work computers. There was no written policy or training about removable media use. A new volunteer frequently used their own USB stick.

Problem: One day, a staff member found a USB drive in the office car park (likely dropped by someone). Curious, they plugged it into their office computer and opened a document on it. That USB was infected with malware. The malware quickly spread through the CSO's network, encrypting files on multiple computers. The CSO's data was inaccessible, and operations were disrupted. The lack of an incident response plan caused confusion: nobody knew who would lead the response or whom to notify.

Outcome: After containing the outbreak by disconnecting affected machines, the CSO engaged an IT specialist to recover data from recent backups. They realized backups helped restore most data. The CSO then implemented strict policies: a formal Acceptable Use Policy was written (forbidding use of unapproved USB drives and requiring a scan of any external media), and the entire staff underwent training on recognizing suspicious devices and attachments. They also developed a simple incident response plan, assigning a response team and clear steps to follow in a future incident (including who to call first and how to communicate with stakeholders). Later, during a minor phishing incident, the CSO successfully contained it using the new plan, minimizing damage.

Discussion Questions:

- *What policies or practices were missing that allowed this incident to occur?*
- *How did having recent backups and a response team affect the outcome of the incident?*
- *Which new measures and plans did the CSO implement after the event, and why are they important for preventing future incidents?*

Module 7 Assessment Note

This module will be assessed with five short questions and one small task. A minimum score of 70% is required to pass.

Module 7 - Assessment

Short Questions

1. What does a "security culture" mean in a CSO context, and why is staff involvement essential to building it?
2. Why are basic IT security policies (such as Acceptable Use or BYOD policies) important for CSOs?
3. How can regular staff training and awareness activities reduce cybersecurity risks in an organization?
4. What are the key elements of a simple incident response plan for a CSO?
5. Why is it important to review and learn from cybersecurity incidents after they occur?

Practical Task: Mini Security Culture Action Plan

Participants are asked to complete the following task:

- Identify one concrete action their CSO could take to strengthen its security culture (e.g., introducing a simple Acceptable Use Policy, organizing an annual security training, or defining an incident response contact person).
- Briefly describe:
  - » Who would be responsible for this action,

» How would it be communicated to staff,

» How it would help prevent or reduce cybersecurity incidents.

Participants should present their answers in three to five short bullet points or discuss them briefly in small groups.

3.8 MODULE

8: ADVANCED TOPICS – EMERGING THREATS AND TOOLS

By the end of this module, the participant will be able to:

- *Recognize sophisticated cyberthreats (like targeted phishing and spoofing) and apply verification methods (such as confirming requests through alternate channels).*
- *Utilize advanced security tools appropriately (e.g., hardware security keys for critical accounts, network monitoring for anomalies, threat intelligence resources).*
- *Plan for organizational security enhancements (like deploying enterprise password managers or intrusion detection systems) based on the CSO's capacity and needs.*

Learning Objectives:

- Become familiar with emerging or sophisticated cyberthreats (such as advanced phishing techniques or spoofing attacks) and learn verification methods to counter them.
- Explore advanced security tools and practices that can further enhance protection, including hardware-based security (e.g., security keys), network monitoring, and threat intelligence, tailored to CSOs' needs.
- Consider how to implement organization-wide security improvements like enterprise password managers or intrusion detection systems, understanding when these advanced measures are appropriate for a CSO's capacity.

Key Topics:

- **Sophisticated phishing & spoofing:** Understanding high-level social engineering attacks (CEO fraud emails, cloned websites, etc.) and learning techniques to verify communications (for example, verifying suspicious requests via a secondary channel or using digital signatures).
- **Hardware security keys:** Introduction to physical authentication tokens (like U2F/FIDO2 keys) as an alternative to SMS or app 2FA. How they work to prevent account takeovers (phishing-resistant 2FA), and considerations for deploying them to staff.
- **Network monitoring and intrusion detection:** Basic concepts of how a CSO could monitor its network for unusual activity. Explaining tools like intrusion detection systems (IDS) or intrusion prevention systems (IPS) in simple terms, and how they alert admins to potential breaches.
- **Organization-wide security tools:** Implementing advanced tools like password managers for the whole organization (to ensure all staff use strong, unique passwords), or utilizing threat intelligence feeds/community alerts to stay updated on new threats relevant to civil society.
- **Tailoring to your context:** Emphasizing that these advanced measures are optional and should be scaled to the CSO's technical expertise and resources. Guidance on how to decide which advanced tools are worth adopting and ensuring staff are trained to use them effectively.

Sample Activities or Exercises:

- **Spear-Phishing Scenario:** The facilitator presents an example of a highly targeted phishing attempt (for instance, an email that looks like it's from a known funder asking for a transfer). Participants practice a verification step (like calling the sender's official phone number or checking the email header) instead of responding via email. Discuss how this approach can thwart sophisticated scams.
- **Hardware Key Demo:** Participants get to see or try a hardware security key. The trainer walks through registering the key to an account and then logging in using the key. If possible, allow volunteers to attempt the

process on a demo account to demystify how these devices work and highlight their security benefits.

- **Mini Threat Hunt:** Provide a simplified network log or an example alert from a hypothetical intrusion detection system (IDS). Have participants examine the entries to spot anything suspicious (e.g., an unknown IP address making multiple login attempts at odd hours). This gives a taste of how network monitoring tools can reveal anomalies.
- **Local Relevance Discussion:** [Insert an example of an advanced threat or a cybersecurity tool that has gained attention in your country] – Discuss whether this threat or tool is something the CSO should be concerned about or consider using. How can local resources (like national CSIRT advisories or cybersecurity communities) help the CSO tackle such advanced threats?

Module 8 Case Study: CEO Fraud Attempt Thwarted

Context: A CSO was managing a large grant project with multiple international donors. Staff are experienced in basic security but have not dealt with highly targeted attacks. The organization had recently introduced hardware security keys for key managers and reviewed advanced security tools.

Problem: The CSO's financial officer received an urgent email supposedly from the executive director, requesting a large wire transfer to a new vendor for project supplies. The email looked legitimate with no obvious phishing signs. The officer was about to proceed when they remembered to verify the request. They called the director at the office. The director, surprised, said he hadn't sent any email. They immediately realized it was a sophisticated email spoofing attempt (CEO fraud). Because hardware security keys were in place for the director's accounts, the attacker had not compromised the director's login; it was a fake email entirely.

Outcome: The CSO staff blocked any further emails from the attacker's address and reported the attempted fraud. To prevent future attempts, the CSO held a briefing on verifying unusual requests (using separate channels) and updated its incident response checklist to include steps for suspected

phishing. They also decided to roll out security keys more widely for high-privilege accounts. Thanks to these measures, the CSO avoided any financial loss and increased staff confidence that advanced phishing attacks can be detected and prevented.

Discussion Questions:

- *How did the CSO detect and prevent the fraud attempt before funds were lost?*
- *What role did the hardware security keys and verification procedure play in this scenario?*
- *Which advanced security improvements (from this module) did the CSO decide to implement as a result of this incident?*

Module 8 Assessment

This module will be assessed with five short questions and one small task. A minimum score of 70% is required to pass.

Module 8 - Assessment

Short Questions

1. What makes advanced phishing or spoofing attacks more dangerous than basic phishing attempts?
2. What is CEO fraud, and why are CSOs particularly vulnerable to this type of attack?
3. How do hardware security keys differ from traditional two-factor authentication methods, and why are they considered phishing-resistant?
4. What is the purpose of network monitoring or intrusion detection systems in an organization?
5. Why should CSOs carefully assess their capacity and needs before implementing advanced security tools?

Practical Task: Advanced Threat Preparedness Check

Participants are asked to complete the following task:

- Identify **one advanced threat** relevant to their CSO (e.g., CEO fraud, targeted phishing, account spoofing).
- Briefly describe:
  - » One verification step staff should take before acting on suspicious requests,
  - » One advanced security tool or practice that could help reduce the risk (e.g., hardware security keys, password managers, verification procedures),
  - » Whether this measure is feasible for their CSO at present, and why.

Participants should present their answers in three to five short bullet points or discuss them briefly in small groups.

4.1 Legal and Regulatory Framework in Türkiye and Suggestions for CSOs in Türkiye

Scope of the Personal Data Protection Law (KVKK) and its Impact on CSOs

Law No. 6698 on the Protection of Personal Data (KVKK) is the primary legislation regulating the processing of personal data in Türkiye. The Law applies to all natural and legal persons who process personal data, including public institutions, private sector organizations, and civil society organizations (CSOs) (Personal Data Protection Authority [KVKK], 2020).

CSOs typically collect and process personal data relating to their members, volunteers, donors, and employees. Such data may include names, contact details, photographs, donation amounts, and event participation records. Therefore, CSOs also bear obligations as data controllers under the KVKK.

According to the Law, personal data may only be processed for specific, explicit, and legitimate purposes, and must be deleted or anonymized once the purpose of processing ceases. CSOs must act in accordance with these principles in all data collection processes, from membership forms to digital campaigns.

Steps CSOs Must Take to Comply with the KVKK

The main steps CSOs should follow to ensure compliance with the KVKK include:

1. **Preparation of a Data Inventory:** CSOs should identify and document which personal data they process, for what purposes, how long the data are retained, and with whom they are shared.
2. **Obtaining Explicit Consent:** Explicit consent must be obtained for processing activities that are not legally mandatory (e.g., promotional

emails). Consent must be freely given, informed, and revocable at any time.

3. Information Obligation: Individuals whose personal data are collected must be informed in writing about who processes their data, for what purposes, on which legal grounds, and what their rights are.

4. Data Security Measures: Physical (locked cabinets), digital (encryption, antivirus software, access restrictions), and organizational (confidentiality agreements, awareness training) measures must be implemented.

5. VERBIS Registration: CSOs whose activities are limited solely to their own members, volunteers, and donors are exempt from VERBIS registration. However, CSOs with an economic enterprise are required to register in the system (KVKK, 2020).

KVKK Violations and Sanctions

The KVKK provides for administrative fines and, in some cases, criminal sanctions in the event of violations (KVKK, 2020). If CSOs fail to fulfill their data security obligations, they may face substantial fines in cases of data breaches, unauthorized data sharing, or failure to notify violations.

As of 2024, administrative fines range from TL 25,000 ($569) up to TL 1,800,000, depending on the nature of the violation. For example, failure to register with VERBIS by a CSO subject to the registration obligation constitutes a serious violation.

The KVKK Board has imposed sanctions on CSOs as well. In 2020, an association was fined following a complaint regarding unauthorized SMS communications, as it failed to provide explicit consent and did not delete the personal data. This demonstrates that CSOs are subject to audits and enforcement measures under the law.

Cybersecurity Law and Notification Obligations

Law No. 7545 on Cybersecurity entered into force as of 2025 and covers all institutions providing services in digital environments, without distinction

between public and private entities (Official Gazette, 2024). Within this framework, CSOs are also subject to incident notification obligations.

In the event of a data breach, malware infection, cyberattack, or the identification of a critical vulnerability within a CSO's systems, the incident must be reported to the Cybersecurity Directorate affiliated with the Turkish Presidency within a maximum of 48 hours.

Failure to comply may result in administrative fines starting from TL 1,000,000 and, in certain cases, criminal sanctions such as imprisonment for responsible persons. This regulation establishes a fundamental obligation of security and transparency for all CSOs.

National Cybersecurity Strategy and the Role of CSOs

The National Cybersecurity Strategy and Action Plan 2024–2028 is the principal document defining Türkiye's digital security vision. The document assigns specific roles to public institutions, the private sector, and CSOs (Ministry of Transport and Infrastructure, 2023).

Key expectations for CSOs include raising public awareness, promoting individual digital security literacy, and conducting digital literacy activities for vulnerable groups such as children and the elderly.

Furthermore, the strategy emphasizes the importance of civil society participation and encourages CSOs to carry out campaigns and training activities in cooperation with public institutions.

Legal Status of Digital Tools

As part of digital transformation, CSOs may be required to use certain digital tools. Under Law No. 5070 on Electronic Signatures, electronic signatures have the same legal validity as handwritten signatures. Board decisions, contracts, and official correspondence may therefore be signed electronically (Information and Communication Technologies Authority, 2023).

CSOs with an economic enterprise or exceeding certain turnover thresholds may be subject to e-invoice (e-Fatura) and e-archive (e-Arşiv)

obligations. The Revenue Administration publishes annual communiques specifying the applicable thresholds (Revenue Administration, 2024).

Registered Electronic Mail (KEP) is another preferred method for official notifications, particularly to ensure legal validity. In using all these tools, CSOs must ensure not only technical adequacy but also full compliance with the relevant legal framework.

Digital Security For Small And Medium-Sized CSOs In Türkiye

Introduction

The following five original cases have been prepared for training purposes and are based on realistic digital security risks and experiences of small and medium-sized civil society organizations (CSOs) operating in Türkiye. Each case clearly presents the structure of the CSO, the incident experienced, the technical or human vulnerability involved, the consequences, and the lessons that can be drawn for other CSOs. All CSOs are presented anonymously in this study.

LOCAL CASE STUDIES FROM TÜRKİYE

Case 1: A Headache Caused by a Fake Email Trap

This CSO is a small educational association operating with only four employees and a few volunteers, aiming to provide scholarships and educational support to local students. Its digital operations rely mainly on email communication, office software, and WhatsApp-based coordination with volunteers. The organization does not have a dedicated IT staff member, and employees generally use their personal laptops for work.

"One day, an email with the subject "Ministry Education Grant" arrives in the association's general info@… inbox. The message claims that the organization has been awarded a grant it applied for and requests that the attached PDF file be opened for further details. Excited by the news, the project officer downloads and opens the attachment without verifying its authenticity. The file does not open properly, but a malicious software is silently installed on the computer."

The main vulnerability in this case is human error and a lack of awareness. The staff member had not received cybersecurity training and failed to carefully examine the sender address, language errors, and suspicious attachment. These were clear indicators of a phishing email designed to impersonate an official institution.

Within a day, shared email accounts used by the project officer and the board were compromised. Attackers sent fraudulent messages requesting money to donors and partners. Communication was disrupted, trust was shaken, and some supporters temporarily suspended their engagement. In the medium term, the organization had to invest time and effort to restore credibility and internal morale.

Lessons Learned and Recommendations

Phishing attacks are one of the most common cyberthreats for CSOs. All staff and volunteers should be trained to identify suspicious emails. Sender addresses, attachments, and urgent requests should always be verified. Basic cyberhygiene practices and two-factor authentication for critical accounts should be implemented.

Case 1: A Headache Caused by a Fake Email Trap

Relevant Module(s)

- Module 4: Common cyberthreats (Phishing & Malware)
- Module 5: Data Protection and Privacy Compliance
- Module 7: Developing a Security Culture

How This Case Can Be Used in Training

- **Awareness-Raising Example (Module 4):**

This case can be introduced at the beginning of the module as a **realistic phishing scenario** targeting small CSOs. Trainers can ask participants to identify red flags in the email (sender address, attachment, urgency, language errors) before revealing the outcome.

- **Human Error Discussion (Module 7):**

Use this case to emphasize that cybersecurity is not only a technical issue but also a **human behavior issue**. It works well as a discussion starter on why training staff and volunteers is critical, especially in small CSOs without IT staff.

- **Account Security Reflection (Module 5):**

The case can support discussion on **email account protection**, including two-factor authentication and access management, linking phishing attacks to broader data protection risks.

Suggested Method:

Group discussion + "What would you do differently?" exercise.

Case 2: Social Media Account Takeover

This case involves a medium-sized women's rights CSO with approximately 20 staff members and volunteers. The organization actively uses social media platforms such as Instagram, X (formerly Twitter), and Facebook for advocacy and public engagement. Accounts are mainly managed by a communications officer, though volunteers occasionally contribute. No two-factor authentication is enabled.

One morning, unusual posts appear on the organization's official Instagram account. The profile picture and biography are changed, and fraudulent investment-related content is shared with followers. Members and followers alert the organization that the account has been hacked.

The communications officer reused the same password across multiple platforms. A data breach on another service exposed the password, allowing attackers to access the social media account. The absence of two-factor authentication further facilitated the takeover. Additionally, the organization lacked a predefined crisis response plan.

The account was temporarily suspended while recovery procedures were initiated. Followers were warned through alternative channels. Although access was eventually restored, reputational damage occurred, and some followers lost trust. In response, the organization strengthened password policies and activated two-factor authentication.

Lessons Learned and Recommendations

Social media accounts are frequent targets of cyberattacks. Strong, unique passwords and two-factor authentication are essential. Password reuse should be avoided, and staff managing social media should receive targeted security awareness training.

Case 2: Social Media Account Takeover

Relevant Module(s)

- **Module 6: Social Media and Online Presence Security**
- **Module 7: Developing a Security Culture**

How This Case Can Be Used in Training

- **Core Case Study (Module 6):**

This case is ideal as a **primary case study** when teaching social media security. Trainers can walk participants through the incident step-by-step and map failures to missing controls (password reuse, no 2FA, no response plan).

- **Incident Response Exercise (Module 7):**

The case can be transformed into a role-play scenario where participants decide how to communicate with followers, report the breach to the platform, and recover the account.

- **Targeted Training Discussion:**

Highlight that staff responsible for communication and advocacy need specialized security awareness, not just general training.

Suggested Method:

Case analysis + incident response role-play.

Case 3: The Cost of Data Loss and Lack of Backups

Type, Scale, and Digital Working Practices of the CSO

This case concerns a small environmental CSO with three full-time staff members and several volunteers. Project documents are prepared on personal laptops and shared via cloud services. However, critical data such as donor lists and financial records are stored only on the director's desktop computer, without regular backups.

Following a power outage, the director's computer fails to restart due to hard drive damage. Attempts to recover the data locally are unsuccessful, and professional data recovery services are recommended at high cost with no guaranteed success.

There was no cyberattack; the incident resulted from poor data management and the absence of a backup strategy. Storing critical data on a single device and using outdated hardware significantly increased the risk of data loss.

OCSOing projects were disrupted, and important reports, financial documents, and contact lists were lost. Staff spent weeks trying to reconstruct missing data. Trust from donors and partners was affected, and financial losses occurred due to recovery efforts and disrupted projects.

Lessons Learned and Recommendations Regular data backups are essential for organizational continuity. Backups should be stored on multiple platforms and tested periodically. Hardware should be kept up to date, and power protection systems should be used.

Case 3: The Cost of Data Loss and Lack of Backups Relevant Module(s)

- **Module 5: Data Protection and Privacy Compliance • Module 7: Developing a Security Culture How This Case Can Be Used in Training • Data Management Example (Module 5):** This case is effective for explaining that not all security incidents involve hackers. Trainers can use it to introduce backup strategies, data availability, and organizational continuity.

• **Risk Assessment Exercise:** » Participants can be asked to list critical data in their own CSOs and identify whether similar single points of failure exist.

• **Leadership Responsibility Discussion (Module 7):** The case demonstrates why data protection and backups are management-level responsibilities, not just technical tasks.

Suggested Method:
Guided reflection + mini data audit activity.

Case 4: The Danger of Weak Passwords and Shared Accounts This scenario involves a medium-sized foundation supporting persons with disabilities. Around 15 staff members and volunteers use shared email and system accounts for daily operations, relying on a single username and password across multiple platforms.

The donor's report receiving suspicious messages requesting money. Investigation reveals that a former volunteer still had access to shared accounts because passwords were never changed after their departure. These credentials were later misused by unauthorized individuals.

Weak and shared passwords, password reuse, and the absence of access revocation procedures created a serious security gap. The organization

lacked clear policies for managing digital access when staff or volunteers leave.

Passwords were changed immediately, and donors were informed. While immediate damage was limited, reputational harm occurred. In the medium term, the organization introduced stronger password policies, individual user accounts, and staff awareness sessions.

Each account should have a strong, unique password. Shared accounts should be avoided where possible, and access rights must be reviewed and revoked promptly when personnel leave. Clear internal policies are essential.

Case 4: The Danger of Weak Passwords and Shared Accounts Relevant Module(s)

- **Module 6: Social Media and Online Presence Security • Module 7: Developing a Security Culture • Module 8: Advanced Topics (Account Access & Controls) How This Case Can Be Used in Training • Policy Gap Illustration (Module 7):** This case clearly demonstrates the risks of missing **access management policies**, especially offboarding procedures, when staff or volunteers leave.

- **Account Security Discussion (Module 6):** Trainers can link this case to the importance of individual accounts, strong passwords, and role-based access – especially for email and donor communication.

- **Advanced Access Control Introduction (Module 8):** The case can serve as a bridge to more advanced practices such as account audits, password managers, and privilege management.

Suggested Method:

Case-based policy drafting exercise (e.g., "What should an offboarding checklist include?").

Trainer's Note (Optional to Add at the End of the Section) These local case studies are designed to:

- Reflect realistic risks faced by CSOs in Türkiye,
- Encourage peer learning and discussion,

• Demonstrate that cybersecurity incidents often stem from simple, preventable issues, • Reinforce the importance of policies, training, and preparedness, not just technology.

Trainers are encouraged to adapt the discussion depth depending on the participants' organizational size, digital maturity, and roles.

Practical Digital Security Policies and Templates for CSOs

Introduction

This document presents practical policy templates that can be used to strengthen the digital security capacity of small and medium-sized civil society organizations (CSOs) in Türkiye. The templates are designed to be simple, actionable, and aligned with both national legislation (the Personal Data Protection Law – KVKK, the Cybersecurity Law) and international good practices (NIST, ENISA, Tactical Tech).

1. Acceptable Use Policy (AUP) Purpose:

To promote the responsible use of organizational digital tools, internet access, and information systems.

Policy Provisions: • All staff shall use the organization's digital resources solely for work-related purposes.

• Passwords must be individual and must not be shared with others.

• Illegal content may not be stored, accessed, or distributed through organizational systems.

• Social media use must not harm the organization's reputation.

• No data may be transferred outside the organization without prior approval from management.

Note:

This policy enters into force upon being signed by staff during onboarding and must be reviewed annually. (ENISA, 2021) **2. Incident Response Plan (IRP)** ***Purpose:***

To ensure a rapid and effective response to potential digital security incidents.

Steps:

1. The person who detects the incident immediately informs the designated authority within the organization.
2. The authority determines the type of incident (phishing, malware, data breach).
3. Affected systems are isolated (removed from the network if necessary).
4. All digital logs and records related to the incident are preserved.
5. The incident is reported to the Cybersecurity Directorate within a maximum of 48 hours (Official Gazette, 2024).
6. A post-incident evaluation is conducted, and procedures are updated accordingly.

Note:

This plan is based on Law No. 7545 on Cybersecurity and NIST SP 800-61 Rev. 2.

3. Basic Data Protection Procedure Purpose:

To ensure that personal data processed within the CSO is managed in compliance with the KVKK.

Implementation:

- Each data processing activity must have a clear purpose and comply with the principle of data minimization.
- Personal data may not be processed without explicit consent, unless otherwise permitted by law (KVKK, 2020).
- For each data-sharing activity, the reason for sharing, the recipient, and the duration must be documented.
- A data retention and destruction policy must be established; personal data must be deleted or anonymized when no longer necessary.
- Paper-based records must be stored in locked cabinets, and digital data must be protected in encrypted folders.

Note:

It is recommended that the organization appoint an internal data controller or responsible person.

4. Credential and Device Sharing Protocol Purpose:
To regulate the secure use and sharing of passwords, user accounts, and digital devices within the organization.

Rules:

- Passwords must be individually assigned and must not be written down.
- On shared devices, each user must log in with a separate account and must not share passwords.
- Transferring data to external devices (e.g., personal laptops) is prohibited.
- The use of USB drives or external storage devices is permitted only with management approval.

Note:
Organizations may additionally define an authentication policy (e.g., multi-factor authentication).

5. Digital Security Commitment (Staff / Volunteers) Commitment Text (Sample): "By this document, I undertake to use the digital systems and tools provided by [Organization Name] solely within the scope of my duties and with due care. I acknowledge my responsibility to fulfil all obligations related to the security of organizational data."
"Bu belgeyle, [Kurum Adı] tarafından tahsis edilen dijital sistem ve araçları yalnızca görev kapsamımda ve dikkatli biçimde kullanacağımı taahhüt ederim. Kurum içi verilerin güvenliği için üzerime düşen yükümlülükleri yerine getireceğimi kabul ederim."

Note:
This commitment should be signed by all staff members and volunteers and retained in their personnel files.

Digital Security Checklists for CSOs To strengthen the digital security of small and medium-sized civil society organizations (CSOs) operating in Türkiye, four separate checklists are provided below. These lists consist of simple and practical items that can be easily applied even by users with limited technical knowledge. Each checklist summarizes essential security steps in line with current legal regulations. The aim is to increase security awareness in daily digital operations and to ensure preparedness for potential emergencies.

1. Basic Digital Security Checklist ¨ Do all users use strong and unique passwords?

¨ Are automatic screen locks enabled on computers and mobile phones?

¨ Is up-to-date antivirus software installed on all devices?

¨ Are all software and applications regularly updated?

¨ Are important documents regularly backed up (external drive or cloud storage)?

¨ Are all users cautious when opening email attachments?

¨ Is the use of external or personal devices monitored?

2. Incident Response Preparedness Checklist ¨ Has a person responsible for digital security been designated?

¨ Is it clearly defined to whom and how incidents should be reported?

¨ Do all staff have basic knowledge of identifying incidents (phishing, malware, etc.)?

¨ Are critical documents and systems backed up?

¨ Is there a written post-incident procedure in place?

¨ Are staff aware of the 48-hour notification rule? (Law No. 7545)

3. Social Media Security Checklist ¨ Do only authorized persons have access to social media accounts?

¨ Is two-factor authentication (2FA) enabled on all accounts?

¨ Are passwords strong and not reused on other platforms?

¨ Is it clear who manages the accounts and for what purpose?

¨ Is the content subject to prior approval before being shared?

¨ Are suspicious logins or unusual follower increases monitored?

4. New Staff / Volunteer Information Security Checklist ¨ Do new staff members or volunteers receive digital security orientation?

¨ Is the Acceptable Use Policy signed?

¨ Are commitments obtained regarding the processing of personal data?

¨ Are access rights limited strictly to job responsibilities?

¨ Are organizational accounts used instead of personal accounts?

¨ Is compliance with organizational password and device policies ensured?

4.2 Legal and Regulatory Framework in Bosnia and Herzegovina and Suggestions for CSOs in BiH

Legal and Regulatory Context in Bosnia and Herzegovina (BiH)

Personal data protection in Bosnia and Herzegovina is governed by the **Law on Protection of Personal Data (Zakon o zaštiti ličnih podataka)**. The competent supervisory authority is the **Personal Data Protection Agency of Bosnia and Herzegovina (AZLP)**. Although the EU General Data Protection Regulation (GDPR) is not directly applicable in BiH, many EU-funded programs and international donors require GDPR-aligned standards. As a result, organizational practices and guidance in BiH increasingly reflect core GDPR principles, such as lawfulness, data minimisation, accountability, and security of processing.

Bosnia and Herzegovina does not yet have a single, comprehensive national cybersecurity law. In this context, Civil Society Organizations (CSOs) are primarily expected to ensure digital security through internal governance mechanisms, including clearly defined roles and responsibilities, internal information security policies, and documented procedures that are consistently applied in daily operations.

National Institutions and Support Mechanisms for cyberincidents

Several public institutions provide support, coordination, or investigative functions in the event of cybersecurity incidents in Bosnia and Herzegovina. These include **CERT BiH**, which is responsible for incident response support, early warnings, and threat monitoring, as well as the **Ministry of Security of BiH – Cybersecurity Sector**, which provides policy-level coordination and guidance. Cybercrime reporting and investigation are handled by the **State Investigation and Protection Agency (SIPA)** through

specialized units, alongside entity and cantonal police cybercrime units responsible for operational investigations at the local level.

Cyberthreat Landscape for CSOs in BiH

Civil Society Organizations in BiH most commonly face cyberthreats related to phishing attacks targeting organizational finances, grants, and donor communication. Ransomware incidents and permanent data loss are also frequent, often due to missing or inadequate backup practices. Impersonation and social engineering attacks are increasingly observed via messaging platforms such as WhatsApp and Viber, while website defacement poses a particular risk for organizations working on politically or socially sensitive issues. In addition, credential theft linked to the use of unsecured public Wi-Fi networks remains a recurring problem.

Operational Reality of CSOs in BiH and Rationale for a Simplified Approach

In practice, many CSOs in Bosnia and Herzegovina rely heavily on personal laptops and mobile phones for organizational work and use platforms such as Gmail, Google Workspace, and social media as their primary operational tools. Dedicated IT or cybersecurity staff are rare, and informal practices such as password sharing within teams are still common.

Given this reality, the curriculum adopts a deliberately simplified and pragmatic approach. It prioritizes low-cost and easily implementable security measures, provides practical templates and ready-to-use documents, and focuses on clear, step-by-step checklists designed for non-technical staff rather than complex technical solutions.

Alignment with European Policy Frameworks

Although Bosnia and Herzegovina is not a member of the European Union, many CSOs operate within EU-funded programs and European policy frameworks. This curriculum is therefore aligned with core GDPR principles, particularly the risk-based approach, as well as broader European cybersecurity awareness and capacity-building strategies. The alignment is

practical rather than legalistic, focusing on day-to-day implementation and organizational behavior instead of formal compliance requirements.

Risk-Based Approach and Policy Logic

European policy frameworks emphasize proportionality, contextual awareness, and impact assessment. The curriculum applies this logic by prioritizing high-risk assets and activities, avoiding overly complex or resource-intensive controls, and focusing on human-centered and realistic security practices that can be sustained within CSO environments.

ISO-Inspired Logic (Simplified)

Even without formal certification, CSOs can benefit from simplified principles inspired by ISO information security standards. These include identifying key organizational assets, applying basic access control principles, establishing structured incident management processes, and promoting continuous improvement through review and learning. This approach supports gradual strengthening of organizational maturity and resilience over time.

Local Case Studies from Bosnia and Herzegovina

Case 1: Phishing Link Leading to Full Account Takeover

This case involves a youth Civil Society Organization based in Sarajevo. The organization operates with a small team and relies heavily on shared email inboxes and social media platforms such as Facebook and Instagram for communication, coordination, and public outreach. Passwords are shared internally, and no two-factor authentication is enabled. A staff member received a Facebook Messenger message that appeared to come from a trusted project partner. The message requested confirmation of details for a joint activity and included a link. The staff member clicked the link and entered the organization's email credentials. Within minutes, the attacker gained access to the shared email inbox and connected social media accounts. Recovery contact details were changed, and fraudulent payment requests were sent to donors.

The incident was enabled by multiple weaknesses, including shared passwords, password reuse across platforms, a lack of two-factor authentication, and excessive administrative privileges for all users. The message was trusted without independent verification. In the short term, the organization lost access to its email and social media accounts, disrupting communication and fundraising activities. Fraudulent messages damaged donor trust. In the medium term, the CSO had to invest significant time in account recovery and rebuilding credibility.

Lessons Learned and Recommendations

All organizational accounts should use unique passwords managed through a password manager and have two-factor authentication enabled. Administrative privileges must be limited, and sensitive requests should always be verified through a secondary communication channel.

Relevant Module(s) and Use in the Curriculum

- **Module 1 – Fundamentals of Cybersecurity:**

Used as a core example to illustrate phishing attacks, credential theft, and rapid account takeover.

- **Module 4 – Common cyberthreats (Phishing & Malware):**

Demonstrates how social engineering exploits trust and a lack of verification.

- **Module 7 – Developing a Security Culture:**

Supports discussion on staff awareness, password hygiene, and the importance of two-factor authentication.

Suggested Use:

Case analysis followed by identifying red flags and mapping preventive controls.

Case 2: WhatsApp/Viber Impersonation Leading to Financial Loss

This case concerns a medium-sized CSO that frequently uses WhatsApp and Viber for internal coordination and financial communication. Sensitive decisions are often handled informally through messaging applications.

An attacker created a WhatsApp or Viber account using the name and profile photo of a real project coordinator. The attacker contacted finance staff with an urgent message stating that bank details had changed and requested immediate use of a new IBAN. The request was processed without verification.

The organization relied on informal messaging platforms for sensitive financial decisions and lacked secondary verification mechanisms. There was no requirement for multi-person approval for financial transactions.

Funds were transferred to the attacker and could not be recovered. The incident resulted in financial loss and internal distress, as well as reputational concerns with donors and partners.

Financial exchanges should never be approved via messaging platforms. All payment-related requests must be verified through official channels, such as signed emails from the organizational domain or phone calls to known numbers. A two-person approval rule should be implemented for significant financial transactions.

Relevant Module(s) and Use in the Curriculum

- **Module 2 – Communication and Social Engineering:**

Primary case illustrating impersonation and urgency-based manipulation via messaging platforms.

- **Module 7 – Developing a Security Culture:**

Highlights the need for internal rules, verification procedures, and shared responsibility for financial decisions.

Suggested Use:

Role-play exercise on verifying urgent financial requests and applying the two-person approval rule.

Case 3: Credential Theft via Public Wi-Fi

This case involves a CSO that allows volunteers to work remotely using personal devices. Cloud services such as Gmail and Google Drive are central to daily operations, and there is no formal policy regulating remote access or device security.

A volunteer worked from a cafe using free public Wi-Fi and logged into the organization's email and cloud storage. The device lacked recent security updates, and passwords were saved in the browser. Shortly afterward, unknown logins were detected, and donor contact lists were downloaded. The response was delayed due to unclear reporting procedures.

The organization allowed access to sensitive accounts over unsecured public Wi-Fi, used outdated devices, and permitted browser-saved passwords. There was also no clear internal incident reporting mechanism.

Sensitive data was exposed, and donor trust was put at risk. Delayed response increased the potential impact of the breach.

Sensitive accounts should not be accessed over public Wi-Fi without a VPN. Devices must be kept up to date, auto-connect features disabled, and incident reporting procedures clearly communicated to all staff and volunteers.

Relevant Module(s) and Use in the Curriculum

- **Module 3 – Devices and Infrastructure Security:**

Core example for risks related to public Wi-Fi, unpatched devices, and insecure credential storage.

- **Module 7 – Developing a Security Culture:**

Reinforces the importance of clear incident reporting procedures and staff awareness.

Suggested Use:

Group discussion followed by a checklist exercise on safe remote working practices.

Case 4: Ransomware via Email Attachment

This case concerns a regional CSO using shared office laptops and email-based document exchange. Backup practices were informal, and no offline backups were maintained. An email resembling a donor report was received, and a staff member opened the attachment on a shared laptop. Shortly after, files became inaccessible, and a ransom note appeared on the screen. The organization trusted the appearance of the sender, lacked attachment

filtering rules, and did not maintain offline or isolated backups. Financial records and project documentation were permanently lost. OCSOing projects were disrupted, and recovery costs were incurred. CSOs should maintain at least one offline backup and use cloud services with version history enabled. Macro-enabled and executable attachments should be restricted, and staff should be trained not to open unsolicited files.

Relevant Module(s) and Use in the Curriculum

- **Module 4 – Common cyberthreats (Malware & Ransomware):**
  Demonstrates how ransomware spreads through email attachments and the impact of missing backups.

- **Module 5 – Data Protection and Privacy Compliance:**
  Highlights data availability, backup obligations, and organizational continuity risks.

Suggested Use:
Scenario-based discussion on backup strategies and "what would you do first?" response steps.

Case 5: Hijacked Facebook Page Due to Shared Logins

Several youth CSOs shared a single Facebook login among staff and volunteers to manage public pages. Access was not reviewed when volunteers left the organization. A former volunteer retained access to the shared account and later misused it. The Facebook page was hijacked and used to publish scam messages and political content. Shared credentials, lack of role-based access, and failure to revoke access when personnel left created a major security gap. The organization's reputation was damaged, and donors contacted the CSO to verify the legitimacy of the posted content. Recovery required time and public clarification.

Lessons Learned and Recommendations

Shared logins should be avoided. Access must be granted through platform role features, two-factor authentication should be mandatory for

administrators, and access rights must be reviewed regularly.

Relevant Module(s) and Use in the Curriculum

- **Module 6 – Social Media and Online Presence Security:**

Primary case for shared credentials, role-based access, and account recovery procedures.

- **Module 7 – Developing a Security Culture:**

Supports policy discussions on access revocation and offboarding procedures.

- **Module 8 – Advanced Topics (Access Control Practices):**

Can be referenced when introducing stronger account governance and administrative controls.

Suggested Use:

Case-based policy drafting exercise focusing on social media access management.

PRACTICAL TEMPLATES & CHECKLISTS For Civil Society Organizations (CSOs) in Bosnia and Herzegovina

ANNEX 1 – ACCEPTABLE USE POLICY (AUP)

Template for Small and Medium CSOs in BiH

Document Title: Acceptable Use Policy (AUP)

Applies to: All staff, volunteers, interns, external consultants

1. Purpose

This policy defines the rules for safe and responsible use of CSO devices, user accounts, and data.

2. Accounts and Passwords

- Use unique passwords for each account.
- Do not share passwords via chat groups, messaging apps, or email.
- Enable two-factor authentication (2FA) for email, cloud storage, and social media admin accounts.
- Use a password manager where possible.

3. Devices (Laptops and Mobile Phones)

- Lock all devices with a PIN, password, or biometric protection.

- Enable automatic system and security updates.
- Report lost or stolen devices within 1 hour to the Incident Lead.

4. Email and Links
   - Do not open unexpected attachments or links.
   - Always verify bank or payment changes via a phone call to a known number.
   - Treat urgent or pressure-based messages as high risk.
5. Wi-Fi and Remote Work
   - Avoid using public Wi-Fi for admin or sensitive accounts.
   - Use a mobile hotspot or VPN if available.
   - Disable auto-connect to Wi-Fi networks.
6. Social Media
   - Use page roles instead of shared logins.
   - Keep the minimum number of administrators.
   - Remove access immediately when a staff member or volunteer leaves.
7. Data Handling
   - Collect only necessary personal data.
   - Store personal data only in approved locations (e.g., CSO cloud drive).
   - Do not store beneficiary data on personal devices without encryption.
8. Incident Reporting

   Any suspected security or data incident must be reported immediately using the CSO Incident Response Plan.

Approved by: _____

Date: _____

Next Review Date: _____

ANNEX 2 – INCIDENT RESPONSE PLAN (IRP) Simplified – for Small CSOs

Document Title: Incident Response Plan (Simplified)

1. What Is an Incident

An incident is any event that threatens CSO accounts, devices, data, or reputation, including phishing, account takeover, malware, ransomware, or data leakage.

2. Roles and Responsibilities (Fill in names) Incident Lead: _____

Communications Lead: _____

IT Support (internal/external): _____

Management Approval: _____

3. First 15 Minutes – Immediate Actions • Disconnect the affected device from Wi-Fi or the internet.

- Take screenshots and note the time and affected accounts.
- Inform internal team: "Do not click links. Incident under review."
- Secure email account first (change password and enable 2FA).

4. First 60 Minutes – Containment

- Reset passwords in this order: email, cloud storage, social media, banking or finance tools.
- Log out all unknown or suspicious sessions.
- Remove unknown admins, apps, and integrations.
- Check email forwarding rules.

5. Assessment (Same Day)

- What happened?
- What data may be affected (donors, beneficiaries, minors)?
- Which systems and accounts are impacted?

6. External Reporting (When Required)

- CERT BiH for incident support and alerts.
- SIPA or police cybercrime units if cybercrime is suspected.
- Consult AZLP requirements if a personal data breach is likely and document actions taken.

7. Communication Rules

- Only the Communications Lead issues external statements.
- Share facts only.
- Inform donors or partners if required.

8. Recovery

- Restore systems from backups.
- Update all devices.
- Re-train staff on the incident type.

9. After-Action Review (Within 7 Days) • Which control failed?
   - What must change (2FA, access roles, backups, training)?
   - Update policies and checklists.

ANNEX 3 – DATA PROTECTION RULEBOOK (INTERNAL) Simple Internal Rulebook for CSOs

Document Title: Data Protection Rulebook (Internal)

1. Scope

This rulebook applies to all personal data processed by the CSO.

2. Basic Data Protection Rules

- Process data lawfully and fairly.
- Collect only what is necessary (data minimization).
- Keep data only as long as necessary.
- Apply protection measures such as access control, backups, and 2FA.

3. Approved Data Storage Locations

CSO cloud drive: _____

CSO email system: _____

Local encrypted folder (if needed): _____

4. Access Control

- Only staff who need the data may access it.
- Remove access within 24 hours when someone leaves.

5. Sensitive Data and Minors

When processing data of minors, apply stricter controls and limit access.

6. Data Sharing

- Share data only through approved channels.
- Do not share beneficiary lists via WhatsApp or Viber.
- Use password-protected files for sensitive data.

7. Incident Handling

Any suspected data breach immediately triggers the Incident Response Plan.

Approved by: _____

Date: _____

Next Review Date: _____

ANNEX 4 – PRACTICAL CHECKLISTS

For BiH CSOs with Low IT Capacity Checklist A – Basic Digital Security Checklist (Starter Pack) Accounts

- 2FA enabled for email, cloud, and social media admins.
- Unique passwords used.
- Passwords are not shared in chat groups.

Devices

- Screen lock enabled.
- Automatic updates turned on.
- Antivirus or system defender is active.

Wi-Fi and Remote Work

- Guest Wi-Fi is separated from staff Wi-Fi.
- No admin logins on public Wi-Fi without hot spot or VPN.

Data and Backups

- Cloud version history enabled.
- Weekly backup available (one offline copy if possible).
- Access is removed immediately when someone leaves.

Social Media

- Page roles used.
- Only 1–2 admins.
- Recovery email and phone belong to the CSO.

Checklist B – Incident Reporting Checklist (Internal) When you suspect an incident

- Disconnect the affected device from the internet.
- Take screenshots and note the time.
- Inform the Incident Lead immediately.
- Change email password and enable 2FA.
- Check for unknown logins and email forwarding rules.
- Identify affected data (donors, beneficiaries, minors).
- Decide if external reporting is required (CERT BiH, SIPA, police, AZLP).

Minimum Incident Record
Date and time detected: _____
Detected by: _____
What happened (short description): _____
Affected accounts or systems: _____
Actions taken: _____
Evidence stored in: _____
External reporting completed (yes/no): _____

4.3 Legal, Regulatory, and Operational Framework for CSOs in North Macedonia

Legal and Regulatory Framework in North Macedonia On April 27, 2016, the European Parliament and the Council of the European Union adopted Regulation (EU) 2016/679 on the protection of natural persons about the processing of personal data and on the free movement of such data, repealing Directive 95/46/EC. This marked the beginning of a comprehensive reform process in the field of personal data protection. Following a two-year transition period, the Regulation became applicable across the European Union on May 25, 2018.

This Regulation, commonly referred to as the GDPR, has been fully transposed in the Republic of North Macedonia through the adoption of the Law on Personal Data Protection, which entered into force on Feb. 24, 2020.

The Law on Personal Data Protection regulates seven fundamental principles for the processing of personal data: • lawfulness, fairness, and transparency,

- purpose limitation,
- data minimization,
- accuracy,
- storage limitation,
- integrity and confidentiality,
- accountability.

Non-governmental organizations, as data controllers, are required to apply all principles cumulatively in every instance of personal data processing and throughout the entire data life cycle. Failure to apply any of these principles constitutes a violation of the Law on Personal Data Protection. The main authority responsible for the implementation and supervision of the Law on Personal Data Protection is the Agency for Protection of Personal Data.

In addition, in the field of cybersecurity, the Law on Security of Network and Information Systems, adopted in July 2025, represents the first comprehensive legal framework regulating cybersecurity in North Macedonia. The law is aligned with the European NIS2 Directive and aims to establish a high and common level of protection of network and information systems in both the public and private sectors.

The Ministry of Digital Transformation and the National Computer Incident Response Team (MKD-CIRT), operating within the Agency for Electronic Communications, are responsible for monitoring, coordinating, and responding to cybersecurity incidents. Of relevance to the private sector, including non-governmental organizations, is the transitional implementation period lasting until 2027, during which all entities are expected to progressively comply with the obligations introduced by the law.

Common Threats and Recent Incidents Affecting CSOs Non-governmental organizations in North Macedonia, similarly to other sectors, are highly vulnerable to cybersecurity threats. A key challenge is that many cyberincidents remain unrecognized or unreported, resulting in a lack of comprehensive and reliable incident data. While a significant number of CSOs report being informed about legislative changes and adapting their operational practices accordingly, available data indicate that many organizations have not adopted internal personal data protection acts and have not appointed a personal data protection officer.

Furthermore, the proportion of CSO staff who have received formal training in personal data protection remains very low. Given that CSOs often operate with limited financial resources and face difficulties allocating funds for staff training, it is recommended that structured cooperation mechanisms be established between the Agency for Protection of Personal Data and the non-governmental sector to facilitate access to training opportunities.

A major risk factor for CSOs is their limited budget for investment in data protection and cybersecurity. Many smaller organizations continue to use unlicensed or outdated software, which significantly increases their

exposure to cyberthreats. At the same time, several manuals and guidance documents are available in the Macedonian language that can support CSOs in strengthening their digital security.

The most identified threats include:

• failure to verify senders before clicking on links or opening messages, • limited use of password managers and frequent reuse of similar passwords, • irregular or absent data backup practices, • use of unlicensed and outdated software,

• insufficient security measures for mobile devices, • very low adoption of two-factor authentication.

National Support and Resources Several national institutions, including the Agency for Protection of Personal Data, the Ministry of Digital Transformation, and the Agency for Electronic Communications, provide support and guidance to CSOs aimed at improving digital security and data protection. Nevertheless, further institutional efforts are required, including systematic planning and state-funded initiatives.

Support is also provided through civil society projects funded primarily by foreign donors to increase digital literacy among CSOs and the general population. A notable example is the project "CyberShield: Empowered Citizens for Cyber Resilience," under which three cybersecurity training sessions were delivered in 2025 for organizations working with marginalized groups. As a follow-up, digital security plans were developed for six civil society organizations. These tailored plans aim to ensure systematic implementation of cybersecurity practices, enhancing organizational resilience and indirectly improving service delivery to end users.

Despite these positive examples, limited funding means that only a small number of CSOs are able to benefit from such initiatives. While several manuals and awareness-raising materials are available in Macedonian, broader and more sustainable cooperation between public authorities and CSOs is necessary to expand access to training and capacity-building activities. Increased funding and targeted programs are particularly needed to support direct education and training of CSO staff.

Cultural and Operational Context of CSOs in North Macedonia Most CSOs in North Macedonia operate on a donor- and project-based model and typically have small administrative and operational teams or rely heavily on volunteers. Organizational work is often carried out using personal devices and widely available digital services such as Google Workspace, Dropbox, or Microsoft 365, frequently without proper licensing.

Training and capacity-building initiatives should therefore focus on practical and realistic measures, including: • the advantages of using licensed products and services, • "Think Before You Click" awareness campaigns, • regular data and information backups,

• active and consistent use of two-factor authentication, • securing mobile devices and managing their use, • responsible password practices,

• effective use of cloud-based solutions,

• increased awareness of data-sharing practices.

Digital literacy levels in North Macedonia remain insufficient, including within the CSO sector. Additional funding, resources, and coordinated efforts are required to achieve a higher level of digital security. These efforts should be translated into concrete programs and practical action plans tailored to the actual needs and capacities of civil society organizations.

FIVE:

APPENDIX AND ANNEXES

101 111 0001
1100 00 0001
01 1100 11

Annexes and Ready-to-Use Templates (North Macedonia) ANNEX 1 – Digital Security Landscape for CSOs in North Macedonia This annex reflects the legal, institutional, and operational realities affecting civil society organizations in North Macedonia and supports the localization of the curriculum.

Threat Landscape • Phishing attacks via email and fake institutional messages, • Ransomware incidents and data loss due to missing backups, • Misuse of unsecured personal data,

- Risks related to the use of personal laptops and mobile devices.

Operational Challenges • Low use of password managers and frequent password reuse, • Irregular or missing data backup routines,

- Use of unlicensed or outdated software,
- Insufficient security of mobile devices,
- Limited adoption of two-factor authentication,
- Lack of dedicated funding for digital security measures.

Template: 10 Basic Steps to Increase Digital Protection The following basic steps are recommended for CSOs in North Macedonia: • Install and regularly update antivirus and anti-malware software, • Apply system and software updates immediately,

- Use strong and unique passwords for each account,
- Avoid opening attachments from unknown or suspicious sources, • Enter sensitive data only on encrypted websites,
- Perform regular backups of organizational data,
- Use separate email addresses for different purposes,
- Prevent phishing by manually typing website addresses,
- Remove outdated or unsupported applications,
- Handle personal and organizational data with caution.

Template – Internal Operational Rules for Digital Security Each CSO should adopt a simple internal document defining digital security rules for

staff, volunteers, and visitors. The document should include: • Use unique passwords for each account,

- Do not share passwords via chat applications or email,
- Enable two-factor authentication for email, cloud storage, and social media admin accounts, • Use a password manager where possible,
- Lock all devices with PINs or passwords,
- Enable automatic updates,
- Report lost or stolen devices immediately,
- Verify all bank and payment change requests,
- Use mobile hot spots when working outside CSO premises, • Assign social media access via platform roles only,
- Keep the number of administrators to a minimum,
- Collect and store only necessary personal data,
- Report any security incident immediately to the designated responsible person.

Template – Incident Response Plan (Simplified) When a digital security incident occurs or is suspected, the following steps must be taken: • Disconnect the affected device from the network,

- Preserve evidence related to the incident,
- Inform the internal team,
- Secure the email account first by changing passwords and enabling 2FA, • Reset passwords for all affected accounts,
- Log out unknown or suspicious sessions,
- Remove unknown administrators and connected applications, report incidents to MKD-CIRT, • Report suspected cybercrime to police cybercrime units, • Consult the Agency for the Protection of Personal Data if a data breach is suspected, • Assess the impact of the incident, and restore systems from backups, • Update devices and software,
- Retrain staff,
- Update internal policies and checklists if needed.

Practical Checklists for CSOs in North Macedonia ANNEX 1 – Digital Security Landscape for CSOs in North Macedonia This annex outlines the legal, institutional, and operational context affecting Civil Society Organizations (CSOs) in North Macedonia. It supports the localization of the digital security curriculum by reflecting common risks, capacities, and practical needs of CSOs operating in the country.

Threat Landscape Civil Society Organizations in North Macedonia commonly face the following digital security threats: • phishing attacks via email and fake institutional messages • ransomware incidents and data loss due to missing or inadequate backups • misuse or exposure of unsecured personal data

• risks related to the use of personal laptops and mobile devices for organizational work **Operational Challenges** In practice, many CSOs in North Macedonia experience the following challenges: • Low use of password managers and frequent password reuse, • Irregular or missing data backup routines,

• Use of unlicensed or outdated software,

• Insufficient security of mobile devices,

• Limited adoption of two-factor authentication,

• Lack of dedicated funding for digital security measures.

Ten Basic Steps to Increase Digital Protection The following basic steps are recommended for CSOs in North Macedonia to improve their digital security posture: 1. Install and regularly update antivirus and anti-malware software.

2. Apply system and software updates immediately when available.

3. Use strong and unique passwords for each account.

4. Avoid opening attachments from unknown or suspicious sources.

5. Enter sensitive data only on encrypted websites (HTTPS).

6. Perform regular backups of organizational data.

7. Use separate email addresses for different purposes (e.g., administration, projects, public communication).

8. Prevent phishing by manually typing website addresses instead of clicking links.
9. Remove outdated or unsupported applications from devices.
10. Handle personal and organizational data with caution at all times.

Internal Operational Rules for Digital Security Each CSO should adopt a simple internal document defining digital security rules for staff, volunteers, and visitors. At a minimum, this document should include the following rules: ¨ Use unique passwords for each account.

¨ Do not share passwords via chat applications or email.

¨ Enable two-factor authentication for email, cloud storage, and social media administrator accounts.

¨ Use a password manager where possible.

¨ Lock all devices with PINs, passwords, or biometric protection.

¨ Enable automatic system and application updates.

¨ Report lost or stolen devices immediately.

¨ Verify all bank and payment change requests through a secondary channel.

¨ Use mobile hot spots when working outside CSO premises.

¨ Assign social media access via platform role features only.

¨ Keep the number of administrators to a minimum.

¨ Collect and store only necessary personal data.

¨ Report any security incident immediately to the designated responsible person.

Incident Response Plan for CSOs in North Macedonia When a digital security incident occurs or is suspected, the following steps should be taken in order: 1. Disconnect the affected device from the network.
2. Preserve evidence related to the incident (screenshots, logs, messages).
3. Inform the internal team and the designated responsible person.
4. Secure the email account first by changing passwords and enabling two-factor authentication.
5. Reset passwords for all affected accounts.

6. Log out unknown or suspicious active sessions.
7. Remove unknown administrators and connected applications.
8. Report incidents to **MKD-CIRT**.
9. Report suspected cybercrime to police cybercrime units.
10. Consult the **Agency for the Protection of Personal Data** if a personal data breach is suspected.
11. Assess the impact of the incident.
12. Restore systems and data from backups where possible.
13. Update devices and software.
14. Retrain staff and volunteers if needed.
15. Update internal policies and checklists based on lessons learned.

ANNEX 2: Basic Digital Security Checklist

Activity/Measure	Checked (Y/N)
2FA enabled for all online outlets	
Unique passwords used for different accounts	
Passwords are not shared in digital form	
Screen lock is enabled on all devices	
Automatic updates turned on	
Antivirus enabled and updated	
Staff Wi-Fi separated from Guest	
Back-up data enabled	
Different page roles on social media	
Recovery email/phone belongs to the CSO	
Hot spot usage of Wi-Fi of admin devices in public	
Closed and disconnected all devices after work	

ANNEX 3: Incident Reporting Checklist

Activity/Measure	Checked (Y/N)
Affected devices disconnected from the internet	
Evidence from the attack was taken	
Changed email and other social media passwords	

Affected data identified	
Unknown admins/apps removed	
Enabled 2FA	
The internal team was informed about what happened	
Banking and payment details are disabled from the device	
The responsible authority/institution was informed about the attack	

4.3 Legal and Regulatory Framework in Norway and Suggestions for CSOs in Norway

Legal and Regulatory Framework in Norway

Civil society organizations (CSOs) operating in Norway are subject to the EU General Data Protection Regulation (GDPR) and the Norwegian Personal Data Act (Personopplysningsloven), which incorporates and supplements GDPR into Norwegian law. These legal frameworks apply to all organizations that process personal data, including non-profit and volunteer-based organizations, regardless of size. The competent supervisory authority is Datatilsynet, the Norwegian Data Protection Authority.

Norwegia CSOs commonly process personal data relating to beneficiaries, members, volunteers, donors, employees, and, in many cases, vulnerable groups. Such data may include names, contact details, financial information, health-related data, case records, or sensitive background information. As data controllers, CSOs are required to comply with the fundamental principles of data protection law.

Key legal obligations include:

Lawful basis for processing: All personal data must be processed on a valid legal ground such as consent, legitimate interest, contractual necessity, or legal obligation.

Informed consent (where applicable): Consent must be freely given, specific, informed, and revocable.

Transparency: Individuals must be informed about how their data is collected, used, stored, shared, and retained through clear privacy notices.

Data minimization and purpose limitation: Only data strictly necessary for defined purposes may be collected and retained.

Security of processing: CSOs must implement appropriate technical and organizational measures to protect personal data against unauthorized access, loss, or misuse.

Data retention and deletion: Personal data must not be stored longer than necessary; retention periods and deletion routines must be defined.

Processor management: Written data-processing agreements must be maintained with all external service providers handling personal data.

International data transfers: Personal data should preferably be stored within the EU/EEA. Transfers to third countries require valid safeguards such as Standard Contractual Clauses (SCCs) and supplementary measures.

Breach notification: Personal data breaches must be assessed promptly and, where required, reported to Datatilsynet within 72 hours.

Datatilsynet has repeatedly identified common challenges among Norwegian CSOs, including unclear consent routines, insecure cloud storage outside the EU/EEA, lack of documented internal procedures, and excessive data retention.

Ethical Responsibilities in Data Protection

Beyond legal obligations, Norwegian CSOs have an ethical duty to protect the privacy, dignity, and safety of the individuals whose data they process. Many CSOs work with people in vulnerable situations – such as refugees, children, victims of violence, or politically exposed individuals – where data exposure can lead to serious personal harm.

Data breaches may result in:

- Harm to beneficiaries and volunteers,
- Loss of donor, partner, and public trust,
- Legal consequences and financial penalties,
- Reputational damage and operational disruption.

Ethical data handling, therefore, requires a precautionary approach: collecting the minimum necessary data, protecting it effectively, and sharing it only when strictly required.

Building Compliance into Daily Practice

For many Norwegian CSOs, particularly those relying on volunteers and limited IT capacity, compliance must be practical and sustainable.

Effective implementation includes:

- Designating a responsible person for data protection and digital security, even if part-time or combined with another role.
- Developing short and accessible internal documents such as a Data Protection Policy and data-handling guidelines.
- Implementing access control routines, including individual user accounts, role-based access, and timely removal of inactive users.
- Selecting secure storage solutions, preferably EU/EEA-based cloud services for personal data.
- Ensuring data-processing agreements are in place with all external providers.
- Providing regular awareness training for staff and volunteers on phishing, passwords, and secure data handling.
- Maintaining a simple incident response routine covering identification, containment, documentation, and escalation.
- Embedding these routines into everyday operations helps ensure compliance is continuous rather than reactive.

Case Studies from Norway

Case Study 1: Targeted Phishing During a Fundraising Campaign (Oslo, 2023) In 2023, a small humanitarian CSO based in Oslo experienced a targeted phishing campaign during its annual fundraising drive. Attackers created a fake version of the CSO's donation page and sent emails to supporters claiming that the organization had "updated its payment system." Several donors entered their card details before the CSO became aware of the scam. The incident damaged donor trust and required significant time and effort to resolve issues with banks and affected supporters.

A basic combination of security measures – such as two-factor authentication on email accounts, domain monitoring, and staff training on phishing red flags – could have reduced the impact of the incident or prevented the attack entirely.

Discussion Questions:

- What were the main vulnerabilities exploited in this incident?
- Which warning signs could have indicated that the emails and donation page were fraudulent?
- Which basic digital security measures might have prevented or limited the damage?

Relevant Module(s) and Use in the Curriculum • Module 1 – Fundamentals of Cybersecurity:

Used as a foundational example of phishing and trust exploitation targeting donors and supporters.

- **Module 4 – Common Cyberthreats (Phishing & Social Engineering):** Demonstrates advanced phishing techniques, including fake websites and impersonation.
- **Module 6 – Social Media and Online Presence Security:** Can be referenced when discussing organizational reputation, public trust, and secure online fundraising practices.
- **Module 7 – Developing a Security Culture:**

Supports discussion on staff awareness, donor communication protocols, and preventative training.

Suggested Use:
Case analysis followed by a group exercise on identifying phishing red flags in fundraising communications and designing a secure donor communication checklist.

Case Study 2: Website Defacement Due to an Outdated Plugin (Bergen, 2022) In 2022, a small human rights CSO based in Bergen had its WordPress website defaced after attackers exploited an outdated plugin. The homepage was replaced with political propaganda, and the organization lost access to the administrator panel. Because the CSO had no recent website backups, restoring the site took more than two weeks and required external technical assistance. The incident disrupted communication with volunteers and donors and caused reputational concerns.

Routine software updates, strong administrator passwords, two-factor authentication, and automated backups would have significantly reduced the impact of the attack**.**

Discussion Questions:

- What technical and organizational weaknesses contributed to this incident?
- How did the lack of backups affect the organization's ability to recover
- Which preventative measures discussed in the module's key topics could help avoid similar incidents in the future?

Practical Digital Security and Data Protection Checklists for CSOs in Norway Relevant Module(s) and Use in the Curriculum

- **Module 3 – Devices and Infrastructure Security:**

Core case illustrating risks related to outdated software and insecure website infrastructure.

- **Module 5 – Data Protection and Privacy Compliance:** Highlights the importance of data availability, integrity, and backups for organizational

continuity.

- **Module 6 – Social Media and Online Presence Security:** Relevant for discussions on website integrity, reputation management, and content control.
- **Module 7 – Developing a Security Culture:**

Supports awareness of shared responsibility for updates and maintenance, not just "IT tasks."

Suggested Use:

Scenario-based discussion followed by a practical checklist exercise on website maintenance, update routines, and backup planning.

ANNEX-1: Legal and GDPR Compliance Checklist for CSOs in Norway

¨ All personal data processed by the organization is identified and documented.

¨ A lawful basis for each processing activity is defined and recorded.

¨ A Privacy Notice/Data Protection Policy is available and communicated.

¨ Consent mechanisms are clear and revocable where required.

¨ Data retention periods are defined and applied.

¨ Data-processing agreements exist with all external service providers.

¨ Personal data is stored within the EU/EEA or protected by valid safeguards.

¨ A data breach notification routine exists, and the 72-hour rule is known.

ANNEX-2. Basic Digital Security Checklist ¨ Strong, unique passwords are used for all organizational accounts.

¨ A password manager is in use.

¨ Two-factor authentication is enabled on email, cloud, and social media accounts.

¨ Devices are protected with screen locks and strong PINs/passwords.

¨ Operating systems and applications are updated automatically.

¨ Antivirus/anti-malware software is installed and up to date.

¨ Critical data is backed up regularly and securely.

ANNEX -3. Cloud and Account Management Checklist ¨ Individual user accounts are used; shared logins are avoided.

¨ Access rights are role-based and limited to necessity.

¨ Inactive accounts are promptly removed.

¨ Cloud access permissions are reviewed periodically.

¨ Sensitive files are shared with restrictions and expiry limits.

¨ Activity logs are enabled where available.

ANNEX-4. Social Media and Online Presence Checklist ¨ Two-factor authentication is enabled on all social media accounts.

¨ Administrator roles are assigned individually.

¨ Recovery email addresses and phone numbers are up to date.

¨ Admin lists are reviewed regularly.

¨ A response plan exists for account hijacking or impersonation.

¨ Website CMS and plugins are regularly updated.

ANNEX-5. Incident Response and Reporting Checklist ¨ A security-responsible person is designated.

¨ Staff know how to report suspected incidents internally.

¨ A written incident response procedure exists.

¨ Evidence and logs are preserved after incidents.

¨ Serious cyberincidents are reported to NorCERT when appropriate.

¨ Personal data breaches are reported to Datatilsynet when required.

¨ Lessons learned are documented and procedures updated.

ANNEX-6. Staff and Volunteer Awareness Checklist ¨ New staff and volunteers receive security and privacy orientation.

¨ Acceptable Use and Data Protection policies are acknowledged.

¨ Regular refresher training is provided.

¨ Clear rules exist for using personal devices for CSO work.

¨ Sensitive data is not shared via insecure channels.

Suggestions and Practical Recommendations

Norwegian CSOs should prioritize simple, well-documented routines over complex technical solutions. By combining clear internal policies, basic technical safeguards, regular training, and ethical awareness, organizations can significantly reduce their digital risks while maintaining compliance with GDPR and Norwegian law.

Additional Norway-Specific Points CSOs Should be Aware of

1. Volunteer Turnover and Access Lifecycle Management

Norwegian CSOs rely heavily on short-term volunteers, interns, and part-time staff. One of the most common risks reported by Datatilsynet and NSM is failure to revoke access when individuals leave the organization.

What CSOs should know:

- Every onboarding must have a corresponding offboarding checklist,
- Accounts, email access, cloud folders, and social media roles must be removed immediately,
- Shared accounts dramatically increase risk in volunteer-based organizations,
- This point strengthens Module 7 (Security Culture & Policies).

2. National Identity Numbers and Sensitive Identifiers

Some Norwegian CSOs process fødselsnummer (national identity numbers), health data, asylum-related information, or legal case details.

Why this matters:

- These data types require higher protection standards under GDPR,
- Storage in unsecured spreadsheets or general cloud folders is a high-risk practice,
- Encryption and strict access control are essential,

• This fits naturally under Module 5 (Data Protection & Privacy), but can be cross-referenced in Module 7 training.

3. Cloud Services and Schrems II Awareness

Many Norwegian CSOs use global cloud services (Google, Microsoft, Dropbox) without understanding data transfer implications.

Norway-specific reality:

• Datatilsynet expects CSOs to be aware of EU/EEA data residency,
• Transfers outside the EU/EEA require safeguards (SCCs + risk assessment),
• "We use a big provider" is not a sufficient justification,
• This strengthens Module 8 (Advanced Topics) with a legal-technical angle.

4. Coordination Between NorCERT and Datatilsynet

CSOs often confuse who to report what to.

Clear distinction CSOs should know:

• NorCERT (NSM): serious cybersecurity incidents (ransomware, account takeover, service disruption),
• Datatilsynet: personal data breaches (GDPR – within 72 hours),
• Some incidents require both notifications,
• This is a key addition to Module 7 (Incident Response & Reporting).

5. Psychological Safety and "No-Blame" Reporting Culture

Norwegian organizational culture strongly values trust and flat hierarchies – but this can backfire if staff fear embarrassment.

Best practice:

• Staff should be encouraged to report mistakes (clicked phishing link, lost device) immediately,

- No-blame culture reduces damage and improves response time,
- This is an important cultural layer for Module 7 that goes beyond technical controls.

6. Board Responsibility and Governance Oversight

In Norway, boards of CSOs are increasingly expected to understand digital risk as part of good governance.

What boards should know:

- Cybersecurity and data protection are governance issues, not just IT matters
- Boards should approve basic security policies and incident response plans
- Serious incidents may have legal and reputational consequences for leadership
- This can be added as a governance note under Module 7 or Module 8.

7. Civil Society as a Strategic Target

Norwegian CSOs working on democracy, human rights, foreign policy, or international aid are considered strategic targets, not random victims.

Implications:

- Attacks may be persistent, subtle, and intelligence-driven
- Not all threats aim for money—some aim for surveillance or disruption
- Awareness of NSM threat briefings is critical
- This reinforces Module 1 and Module 8 with a Norway-specific threat model.

APPENDIX

Appendix 1: Glossary of Key Terms

- ***Antivirus (AV):*** *Software that detects and removes malware (viruses, trojans, etc.) from computers. Example: Windows Defender or Avast.*
- ***Backup:*** *An extra copy of data stored separately for recovery purposes, e.g., saving files on an external hard drive or cloud service so they can be restored if originals are lost.*
- ***Brute Force Attack:*** *A method where attackers try many passwords or keys until the correct one is found. Strong passwords and lockout policies help defend against this.*
- ***Data Breach:*** *An incident where sensitive information is accessed or disclosed without authorization. Could occur via hacking, lost devices, etc.*
- ***Encryption:*** *The process of converting data into a coded format that is unreadable without a key. Protects information confidentiality (e.g., HTTPS encrypts web traffic).*
- ***Firewall:*** *A network security device or software that monitors and filters incoming and outgoing network traffic based on security rules. It can block unauthorized access while permitting legitimate communication.*
- ***Malware:*** *Malicious software designed to harm or exploit systems. Includes viruses, ransomware, spyware, etc. Often delivered via email attachments or malicious websites.*
- ***Multi-Factor Authentication (MFA / 2FA):*** *Using more than one verification method to log in (e.g., password + one-time code on phone). Dramatically improves account security.*
- ***Phishing:*** *A fraudulent attempt (usually via email) to trick individuals into revealing sensitive information or installing malware by posing as a trustworthy entity. Spear phishing refers to targeted attempts at specific individuals or organizations.*
- ***Ransomware:*** *Malware that encrypts a victim's data and demands payment for the decryption key. If no backups exist, victims face pressure to*

pay hackers to regain access.

- ***Social Engineering:*** *Tactics that manipulate people into divulging confidential info or performing actions that compromise security. Phishing is one form; others include pretexting or baiting. It exploits human trust and curiosity.*
- ***VPN (Virtual Private Network):*** *A tool that creates an encrypted tunnel over the internet from your device to a server, protecting data in transit and masking your IP address. Useful on public Wi-Fi for a secure connection.*
- ***Vulnerability:*** *A weakness in software, hardware, or procedure that attackers can exploit to gain unauthorized access or perform unauthorized actions. Patching addresses known vulnerabilities.*
- ***Wi-Fi Encryption (WPA2/WPA3):*** *Security protocols for wireless networks that encrypt traffic between devices and the router. Ensure your Wi-Fi uses at least WPA2 with a strong passphrase to prevent eavesdropping.*

Appendix II: Password Policy Template (Example)

Purpose: To establish requirements for creating, using, and managing passwords to protect the organization's information systems.

Scope: This policy applies to all staff, volunteers, and contractors of [Organization Name] who use IT systems (including computers, email, applications, and websites) for organizational work.

Policy Statements:

- *All user passwords must be at least 12 characters long, mixing upper- and lower-case letters, numbers, and special symbols.*
- *Default passwords must be changed immediately upon first use.*
- *Passwords must not be shared between individuals or written down in insecure locations.*
- *Two-factor authentication (2FA) is required for all remote access to organizational systems and for email accounts.*

- *Passwords for critical systems (financial, donor databases) must be changed every 90 days.*
- *Users must not reuse passwords that have been used on other (public) accounts or leaked in breaches.*
- *If a password is suspected of being compromised, it must be changed immediately, and the IT/security officer must be notified.*

Roles and Responsibilities:

- *Users must follow these rules and report any suspected compromise.*
- *IT staff will enforce password rules through technical controls (e.g., password managers, account lockouts after failed attempts).*
- *The security officer will review compliance and update the policy annually.*

Enforcement: Violations of this policy may result in revocation of access privileges or other disciplinary actions.

Appendix III: Backup Policy Template (Example)

Purpose: To ensure that critical data is regularly backed up and can be restored in case of loss, corruption, or disaster.

Scope: Applies to all data stored on organizational servers, workstations, and network storage devices at [Organization Name].

Policy Statements:

- *Critical data (donor records, financial files, project databases, etc.) must be backed up at least daily.*
- *Backups should include system configurations and applications needed to restore operations.*
- *Backup copies must be stored securely off-site or in a separate cloud storage to prevent loss from local incidents.*
- *Full backups are performed weekly, with incremental backups daily (or more frequently for highly sensitive data).*
- *Backup integrity checks and test restores must be performed monthly to ensure data can be recovered.*

- *Retention: Retain at least one full week of daily backups on-site, and a monthly full backup archived off-site for at least one year.*
- *Access to backup data is restricted to authorized IT or management personnel only.*

Roles and Responsibilities:

- *IT staff must configure and monitor automated backups according to this schedule.*
- *The designated Backup Administrator will document backup procedures and verify backup completion and integrity.*
- *All staff are responsible for saving critical work files in the designated locations that are included in the backup schedule.*

Enforcement: Failure to comply may result in data loss and will be addressed by [Organization Name] management accordingly.

Appendix IV: Asset Inventory Template (Example)

Asset ID	Asset Name	Category	Owner/Department	Location	Sensitivity Level	Protection Required	Notes
A001	Donor Database	Software/Data	Program Director	On-site	High	Encrypted, password-protected	Contains PII of donors
A002	Financial Server	Hardware/Server	IT Department	Data Center	High	Regular backups, 2FA for access	Supports accounting software
A003	Laptops	Hardware/Device	Various Staff	Office/Field	Medium	Enforced disk encryption, password	Each device has an ID tag
A004	Website	Software	Communications	Cloud-hosted	Medium	HTTPS enabled, updated CMS	Public-facing website
A005	CRM Software	Software	Data Manager	Cloud	High	Role-based access, daily backups	Tracks beneficiary info

(Note: 'Sensitivity Level' can be Low/Medium/High. 'Protection Required' outlines security measures for each asset.)

Appendix V: Simple Risk Matrix Template (Example)

	Impact: Low (1)	**Impact: Medium (2)**	**Impact: High (3)**
Likelihood: High (3)	High Risk (3×1)	Critical Risk (3×2)	Critical Risk (3×3)
Likelihood: Medium (2)	Medium Risk (2×1)	High Risk (2×2)	Critical Risk (2×3)
Likelihood: Low (1)	Low Risk (1×1)	Medium Risk (1×2)	High Risk (1×3)

Risk Levels: Calculate risk by multiplying likelihood and impact scores. For example, a scenario rated Likelihood=3 (High) and Impact=2 (Medium) yields a risk score of 6 (Critical Risk).

- Use this matrix to prioritize addressing higher-risk scenarios first (Critical > High > Medium > Low).

CONCLUSION

Digital security is not a one-time project or a box to be checked – it is an oCSOing commitment. As we conclude this e-book, we want to reaffirm a central lesson that has echoed through every chapter: keeping our civil society organizations safe online requires continuous attention, adaptation, and care. The cyberthreat landscape we discussed at the start is constantly evolving, with attackers daily seeking new ways to breach defenses. What we secure today may be tested by new tactics tomorrow.

This reality means that digital safety must remain on our radar for the long haul, as integral to our planning and operations as budgeting or program management. We cannot afford to treat cybersecurity as an afterthought; rather, it should become a habitual part of how we work. The stakes are simply too high – when a single successful hack can expose sensitive beneficiary data or derail an advocacy campaign, vigilance in digital security is part and parcel of fulfilling our missions. The knowledge and strategies you have gained from this e-book are a foundation to build upon. Going forward, staying safe will mean regularly revisiting these topics, updating your practices as new threats (and solutions) emerge, and fostering an environment where learning about security is a continuous process. In short, the work of digital security is never "finished," but neither is it insurmountable. With each step you take to reinforce your organization's cyberdefenses, you are contributing to a more resilient civil society.

Maintaining Security Made Easy: One key takeaway is that security doesn't have to be overly complicated. Often, it's about doing the simple things consistently. Use strong, unique passwords (and a password manager). Keep your software updated. Think twice before clicking unexpected links. Back up your data regularly. These basic practices, when ingrained, handle a large percentage of threats. As we saw, many attacks succeed due to overlooked basics – so by tending to these, you close the common doors that attackers exploit.

Adapting to New Challenges: The digital world will continue to change. Five years ago, ransomware wasn't as dominant; today it's a top threat. In the future, we might contend with attacks on artificial intelligence tools or more sophisticated deepfake phishing. Your CSO should remain adaptable and keep learning. Subscribe to a relevant security feed or join a community where new threats are discussed – that way, you get early warning of emerging issues. Consider periodic refresher training or new modules for staff when something significant changes (for example, if mobile malware surges, do a special session on that). Embrace a mindset of continuous improvement, treating each near-miss or incident as a learning opportunity to strengthen defenses further.

Allocating Resources Wisely: Security is an investment in your organization's sustainability. It might require some budget (for better equipment, software, or training time) and management attention. But as demonstrated, the cost of not securing (breaches, downtime, lost trust) is far higher. Plan for security in your long-term strategy – e.g., include a line in grants for technology updates or training. Leverage free or discounted services for CSOs (there are many, from free Google Workspace to donated firewalls) as discussed in Chapter 6. Also, consider designating a security point person (even if not full-time) who keeps tabs on security tasks and developments – having someone accountable ensures it doesn't fall through the cracks.

Support from Leadership: Sustainable security needs leadership endorsement. When leaders prioritize security – by modeling good practices and allocating resources – it sends a clear message that this is important for everyone. It also counters any pushback (like "do we really need to bother with this?"): if the director is logging in with 2FA and attending the same trainings, it legitimizes the effort. So, ensure your management team is fully on board and even championing security initiatives.

***Engage Your Whole Team*:** A secure future depends on everyone playing a role. From the newest intern to the board members, each person has a part in the chain. Keep security inclusive: encourage questions, don't shame

mistakes, reward vigilance. Some organizations include a security competency in performance reviews or job descriptions, underscoring that it's an expectation for all roles. By empowering staff – giving them knowledge and tools – you've essentially grown a human firewall around your CSO. As one saying goes, "the security awareness of users is the cheapest and most effective firewall you can have."

Looking Ahead with Optimism: It can be easy to feel intimidated by cyberthreats, but remember that knowledge and preparation tilt the balance strongly in your favor. Many CSOs around the world, even under-resourced ones, have successfully defended themselves by being proactive and united. By reading this e-book and implementing its guidance, you have taken an important step toward securing your organization's digital future. It's a journey – there will be bumps and possibly incidents – but each step you take now reduces the impact of those and accelerates your recovery.

In a world where civil society is sometimes specifically targeted by cyberattacks, your commitment to digital security is also a commitment to your cause and the people you serve. It means your important work can continue without being derailed by preventable disruptions. It means the trust people place in you – for handling their data or amplifying their voices – is well-founded.

As we conclude, let's recap a few long-term security habits to cultivate:

- *Regularly revisit your risk assessment and update your security plan (at least annually or when major changes happen).*
- *Keep learning – attend that webinar, read that guide, share insights with peers.*
- *Stay connected – don't isolate your security efforts; be part of the community that learns and defends together.*
- *Be prepared – maintain your incident response plan and test it occasionally so it's ready if needed.*
- *Remain vigilant – but not fearful. With good practices in place, you can be confident and calm, not anxious, about digital threats.*

Toward a Secure Future: By making digital security an integral part of your CSO's daily operations and culture, you are well-positioned to face the future. Challenges will undoubtedly arise, but you have the tools, knowledge, and support to overcome them. In doing so, you protect not just your organization but also contribute to a safer digital environment for the broader civil society.

Moving forward, commit to continuous improvement. Celebrate your security wins (even small ones like "no one fell for phishing this quarter!" or "we successfully restored data from backup after a minor server crash"). Learn from any setbacks. And always remember the why: a secure CSO can better deliver on its mission and make a positive impact without interruption.

Building resilience is another theme we have emphasized, and it deserves to be stressed again here at the conclusion. Resilience means not only trying to prevent attacks but also ensuring that your organization can bounce back if something does go wrong. It's about having backups so a ransomware attack doesn't cripple your operations, about having response plans so a phishing incident can be contained and learned from, and about cultivating an organizational mindset that views setbacks as opportunities to improve. As you carry on with your work, remember that every challenge can make you stronger if met with preparation and reflection. If a security incident occurs, use it as a learning experience to refine your policies and training. Celebrate the progress you've made – for instance, turning that "80% of organizations without a security plan" statistic on its head in your own context by putting a robust plan in place. And continue to educate yourself and your team. The field of digital security evolves quickly, but there are more resources than ever (many of which we've listed in Chapter 7 and the appendices) to keep you updated. Consider periodic refresher workshops, subscribe to alerts or newsletters on cybersecurity for nonprofits, and encourage younger staff or volunteers with IT interests to take on roles as "digital safety champions" within your organization. Continued learning is

the cornerstone of resilience. It keeps you agile and ready to meet whatever the digital world throws your way.

Looking ahead, we remain optimistic and forward-looking about the future of civil society in the digital age. Yes, the challenges are significant – cyberattacks are growing more sophisticated, and we must stay on our toes. But the progress made even in the past few years is encouraging. More organizations are waking up to the importance of digital security, and support structures are slowly but surely strengthening. We are seeing the development of tools and services tailored for nonprofits, increased awareness among donors and institutions about funding cybersecurity needs, and greater global attention to the concept of "digital resilience" for communities. Each chapter of this e-book has not only offered cautionary guidance but also highlighted opportunities – the opportunity to turn technology to our advantage, to innovate in how we protect ourselves, and to shape a digital environment that upholds our values. As we noted, cyberthreats will continue to evolve, but so can our defenses. By bridging remaining gaps in knowledge and capacity, by strengthening partnerships, and by keeping cybersecurity a priority for those who need it most, we can create a safer digital ecosystem where civil society can continue its critical work without fear.

In closing, we want to leave you with an empowering thought: every effort you invest in digital security is an investment in the freedom and integrity of your work and the people you serve. Each new password policy, each encrypted database, each staff training session – they all add up to a stronger shield protecting human rights, social justice, and community welfare initiatives around the world. The fact that you have read this e-book and engaged with these topics is a positive step toward a more secure future. We encourage you to carry this commitment forward. Share what you've learned with colleagues and partner organizations. Keep the conversation about digital safety alive in your strategy meetings and planning sessions. Advocate for the resources and support you need – whether that's funding for better infrastructure or simply time allocated for staff to learn and

implement security measures – because digital security is worth it. The forward-looking view is that by embedding security into our daily work, we do more than just protect our organizations; we enable them to thrive. A secure civil society organization can speak louder, act bolder, and reach further, knowing that its voice cannot be easily silenced by digital threats.

One of the most heartening insights from the KA220 project and this e-book is that we are not alone in facing these challenges. In fact, collaboration is one of our strongest assets. If there is one message to carry forward, it's that we are safer together. Cyberthreats can often feel isolating – a small nonprofit may feel outmatched against a sophisticated hacker – but the collective power of civil society, working in concert, can tilt the balance. Throughout this project, we have been inspired by the examples of organizations teaming up to share expertise, by networks of digital volunteers lending a hand, and by partnerships that have formed across borders to tackle common security issues. The path to digital safety is not a solitary one; it is a shared journey. By communicating openly about threats and incidents, by sharing tools and success stories, and by supporting each other through emergencies, civil society organizations amplify their defense capabilities. Moreover, broad cooperation beyond the nonprofit sector is essential. We need to continue forging partnerships with allies in government, academia, and the tech industry who are committed to protecting the open and safe internet that civil society relies on. As experts and global cyber leaders have noted, defending at-risk groups effectively "demands investment in cybersecurity solutions, collaboration among stakeholders, and innovative funding models for long-term resilience". No single organization – no matter how well-resourced – can address all aspects of digital security alone. It will take a community of practice, spanning different sectors and expertise, to ensure that protective measures are available, effective, and sustainable in the long term. I encourage you to seek out these collaborations: join security forums and coalitions, engage with initiatives that offer cybersecurity assistance to CSOs, and don't hesitate to reach out to peers for help or to offer your own. By strengthening these ties,

we create a united front that can respond to threats swiftly and prevent small issues from becoming large crises.

Thank you for being a part of this journey to develop digital security infrastructure through civil society. The conclusion of this textbook is not an end but rather a beginning – the starting point of new initiatives, conversations, and collaborations that will continue beyond these pages. Stay curious, stay vigilant, and stay united. Together, we will build a digital environment where civil society is not only safe but empowered to leverage technology in defense of the causes we hold dear. With resilience, cooperation, and continuous learning as our guides, we move forward into a future where organizations like yours can confidently embrace innovation and drive social change, supported by a robust foundation of digital security. Let's continue this important work – our communities are counting on it, and the tools and allies we need are within reach. Here's to a safer, stronger, and more empowered civil society in the digital era.

Co-funded by the European Union

Practical Digital Transformation Guide and Curriculum on Strengthening Digital Security in Civil Society was created with one clear purpose: to make digital safety achievable, understandable, and actionable for every organization, regardless of size or technical capacity. As you move forward, we hope this guide serves not only as a resource but as a companion on your journey toward stronger, safer digital practices.

Digital resilience grows step by step, through awareness, collaboration, and consistency. By integrating these practices into your daily work, you are not only protecting data and communication but also defending human rights, trust, and democratic values in the digital age.

Stay aware. Stay resilient. Stay secure.