Digital Security

PROTECTING INDIVIDUALS AND ORGANIZATIONS
IN THE DIGITAL WORLD

TÜRKİYE ULUSAL AJANSI
TURKISH NATIONAL AGENCY

Co-funded by
the European Union

SETA

What is Digital Security?

Digital security is the practice of defending our digital lives from theft, damage, and unauthorized access.

The protective steps that people and companies take to lower the danger of cyberattacks involve safeguarding our everyday gadgets —such as smartphones, laptops, tablets, and computers— along with the online services we use, to prevent theft, physical damage, or illegal access to the massive amounts of personal data we keep.

The Core Goal: CIA Triad

Confidentially

Controlling access
to information.

Integrity

Assuring
information is
reliable and accurate.

Availability

Guaranteeing access
to information
when needed.

Why This Triad Matters?

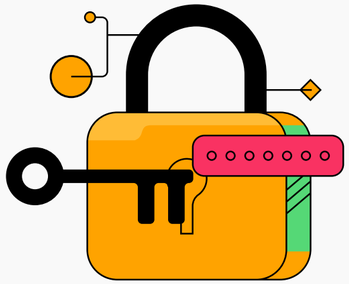
For organizations like NGOs, failing to meet these goals can lead to **"digital fragility".**

1. If **confidentiality** is breached, sensitive beneficiary data may be leaked;
2. If **integrity** is lost, communications could be falsified (such as deepfake voice messages mimicking an executive director);
3. If **availability** is compromised, an organization may be unable to deliver aid or advocate for vulnerable populations.

Understanding the key concepts is the first step to building a strong defense

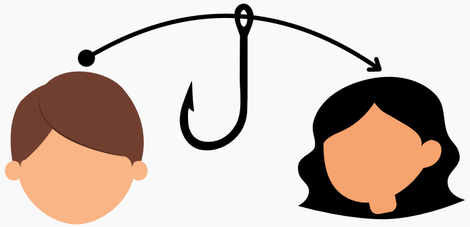
Encryption

The process of converting data into a code to prevent unauthorized access.



Multi-Factor Authentication (MFA)

A security process requiring two or more validation methods to verify a user's identity.

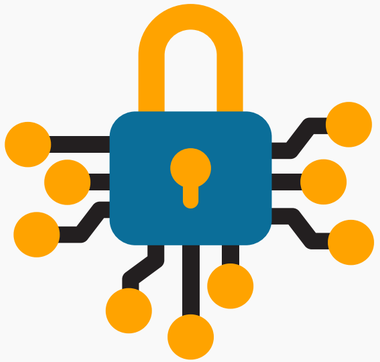


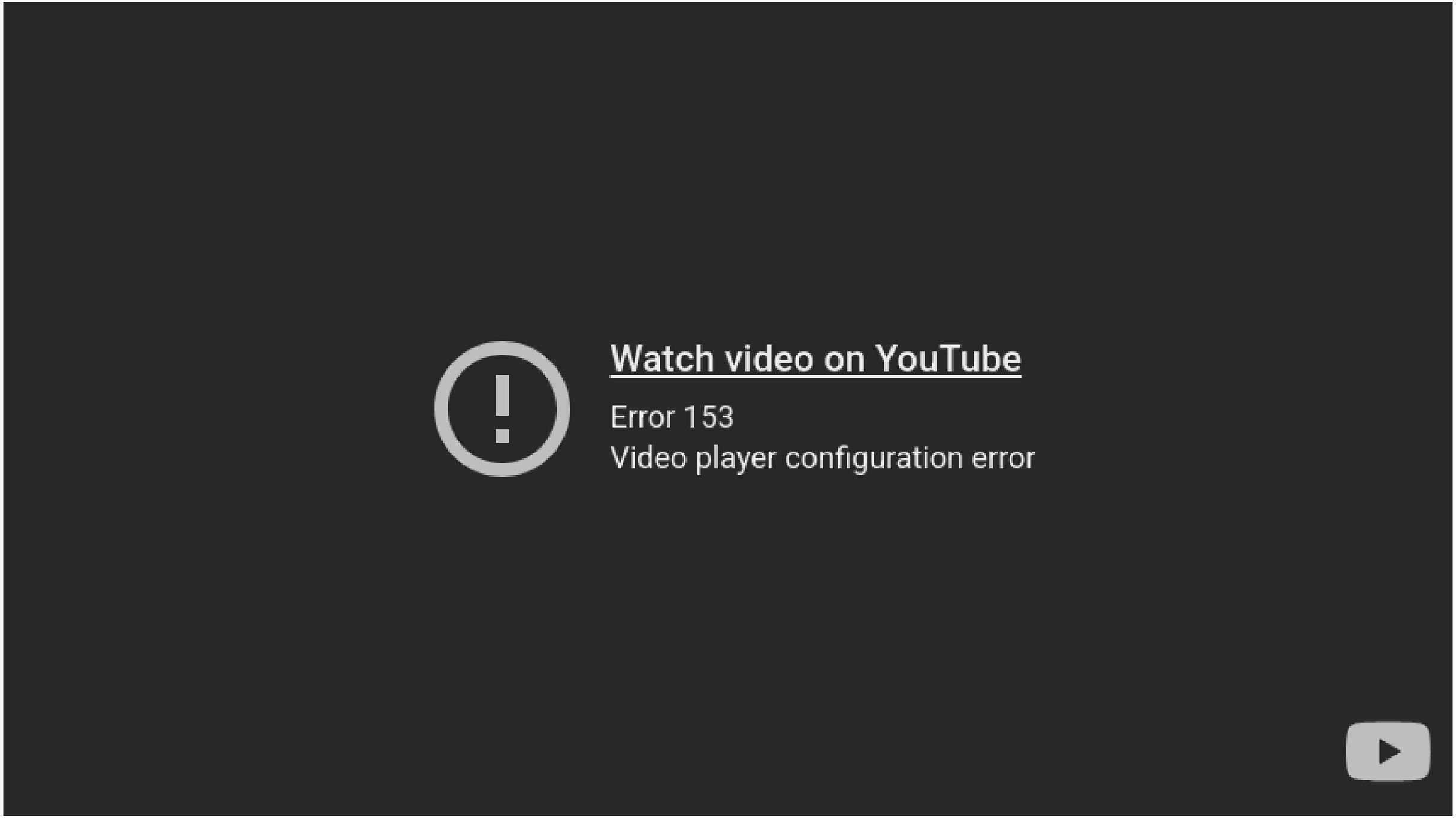
Social Engineering

The psychological manipulation of people into performing actions or divulging confidential information, often through phishing, deepfake voice scams, or other fraudulent means.

Zero Trust

A security model where no user, device, or system is trusted by default. Every access request must be continuously verified.

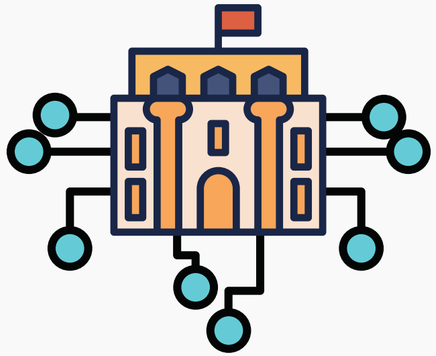



Watch video on YouTube
Error 153
Video player configuration error

Attacks are driven by a diverse set of actors, from organized criminals to nation-states

Cyber Criminals

Primarily motivated by financial gain. Their methods include Ransomware, fraud, and data theft for resale.



Nation-State Actors

Motivated by espionage, geopolitics, and disruption. Their attacks are sophisticated, highly targeted, and increasingly directed at civil society.

Malicious Insiders

Disgruntled or unhappy staff who use their authorized access to carry out malicious activity, causing disruption or reputational damage.

Human Error

Unintentional actions by staff or individuals that create security vulnerabilities, often exploited by external attackers.

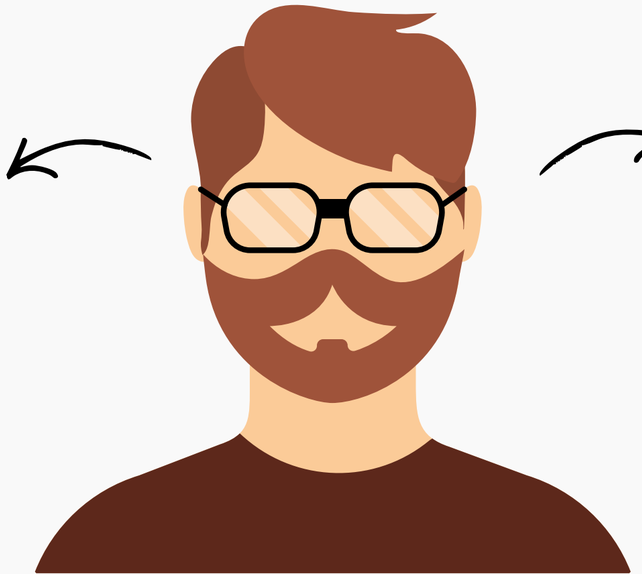
Primary Risks For Individuals

Phishing and Social Engineering

Fraudulent emails and texts, or even AI generated "deepfake" voice calls, designed to trick you into revealing sensitive information.

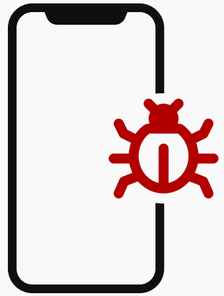
Scamming & Blackmail

Financial fraud through impersonation scams, or extortion based on compromised personal information.



Identity Theft

Attackers using your stolen personal data to open accounts, file fraudulent tax returns, or commit other crimes in your name.



Malware on Personal Devices

Viruses and spyware that steal passwords, financial details, and can even be used to track your movements.

4 Essential Steps to Improve Personal Security

Master Your Passwords

Use a password manager to create long, unique, and complex passwords for every account. Avoid reusing passwords.

Enable MFA

Activate Multi-Factor Authentication (MFA) on all critical accounts (email, banking, social media). This is your single most effective defense against account takeover.

Spot the Phish

Be skeptical of unsolicited messages. Always verify requests for money or sensitive information through a separate channel.

Stay Updated

Regularly update your operating system, browser, and applications to patch security vulnerabilities

Primary Risks For Ogranizations

Ransomware

Harmful software designed to lock up a organization's files using encryption. Cybercriminals frequently pair this with data theft in what are known as 'double extortion' schemes, requiring one payment to unlock the data and a separate payment to ensure that the stolen information is not released to the public.

Data Breaches

Unauthorized access and exfiltration of sensitive data, including customer information, intellectual property, and employee records.

Supply Chain Attacks

Compromising an organization not directly, but through a trusted third-party vendor, managed service provider, or software platform.

Insider Threats

Current or former employees, contractors, or partners intentionally or unintentionally causing harm or data leaks

Effective digital security is not a single product, but a continuous process built on three pillars

Implementing the right tools to protect systems and data (e.g., Firewalls, Encryption, Anti-Malware)

Establishing clear policies, standard operating procedures (SOPs), and plans to guide behavior (e.g., Incident Response Plans, Access Control Policies)

Fostering a culture of security awareness and "cognitive resilienee" through regular, scenario-based training.

1) Identity-First Security (Zero Trust)

- Enforce **Multi-Factor Authentication (MFA)** for all users through a digital service or system, requiring one or more proofs of identity in addition to a password or PIN, such as a code texted to a phone or a response to an app.

- Apply the Principle of Least Privilege (using rolebased access control) so users can only access data essential to their roles.

Physical Tokens

Smart cards and USB tokens (also called security keys), which require a smart card reader and a USB port respectively.

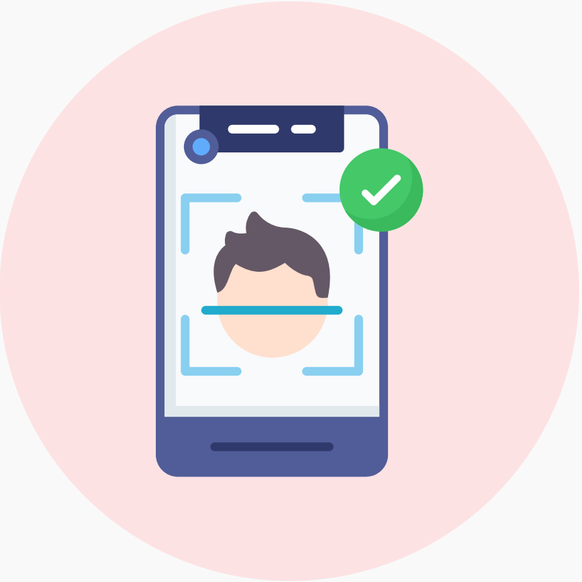
Increasingly, FIDO2 tokens, supported by the open specification group FIDO Alliance have become popular for consumers.

Something the user knows...

Certain knowledge only known to the user, such as a password, PIN, PUK, etc.

Something the user is...

Some physical characteristic of the user (biometrics), such as a fingerprint, eye iris, voice, typing speed, pattern in key press intervals, etc.



2) Encrypt and Back Up Critical Data

- Encrypt sensitive data both at rest (on servers) and in transit (over networks).

- Maintain regular, isolated backups to enable recovery from ransomware. You can use **the 3-2-1 rule** is a data backup strategy that protects your data from hardware failures, cyberattacks, accidental deletion, and natural disasters. It suggests keeping three copies of your data on two different media types, with one copy stored offsite.

	WhatsApp	Telegram	Signal
Base	The U.S.	Dubai (formerly Russia)	The U.S.
Data Privacy	Collects data (phone, usage, habits) and shares with Meta	Privacy-oriented; data is not sold; cloud-based storage	Minimum data collection; only phone number is required
Metadata	Collects metadata (who, when, etc.)	Cloud-based synchronization metadata	Does not collect metadata
Cloud Storage / Backup	Local + Cloud (Google Drive/iCloud); backups are not encrypted by default	All data is stored in the cloud (except Secret Chats)	Local storage; backups are fully encrypted
Default Encryption	End-to-End (E2E) for all chats	Server-client (E2E only in "Secret Chats")	End-to-End (E2E) for all chats, calls, and backups
Open Source Status	Closed source (not auditable)	Partially open source (Client-side)	Fully open source (Auditable by experts)

3) Develop a Security Culture

- Conduct regular, **scenario-based training** that moves beyond compliance checklists. Expose staff to realistic simulations of phishing and social engineering.

- Foster a culture where employees can immediately flag suspicious activity without fear of blame.

4) Plan and Prepare for Incidents

- Develop and test a Cybersecurity Incident Response Plan. Define roles, responsibilities, and the steps to contain damage.

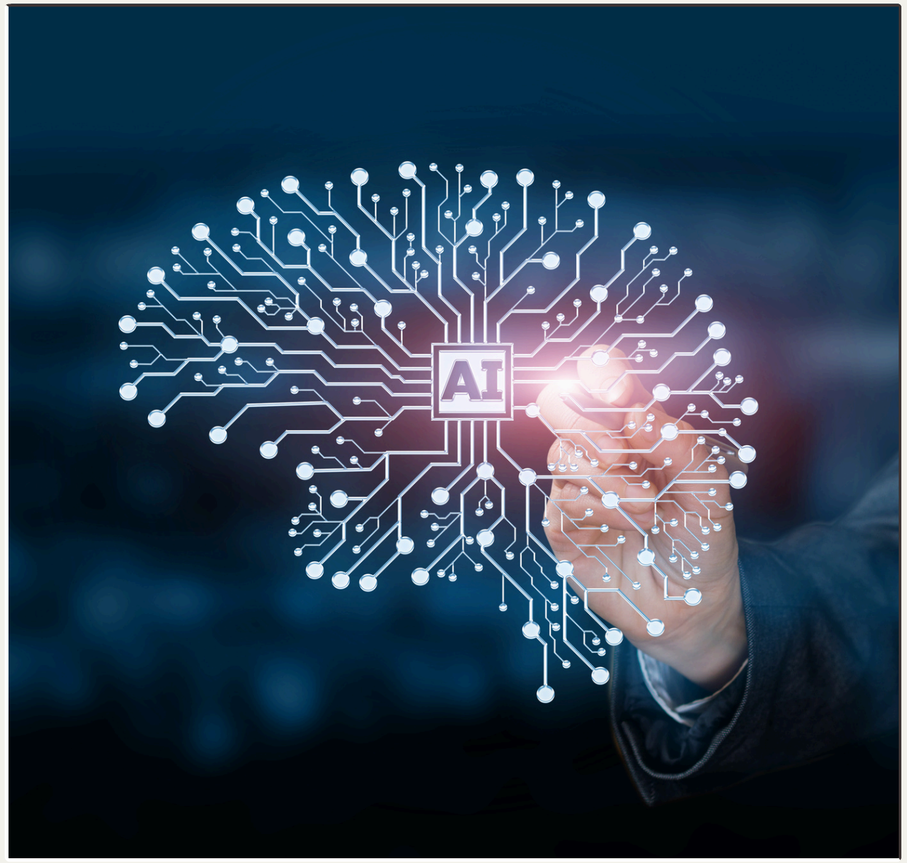
- Assess **third-party risk**. Vet the security practices of your vendors and partners as part of your procurement process.

Preparing for 2026 and Beyond

The AI Double-Edged Sword

AI will be "both the greatest weapon and the strongest shield," powering hyper-personalized attacks (deepfakes, intelligent malware) and sophisticated, automated defenses.

Responsibly adopt AI-driven detection tools while investing in AI literacy for your teams.

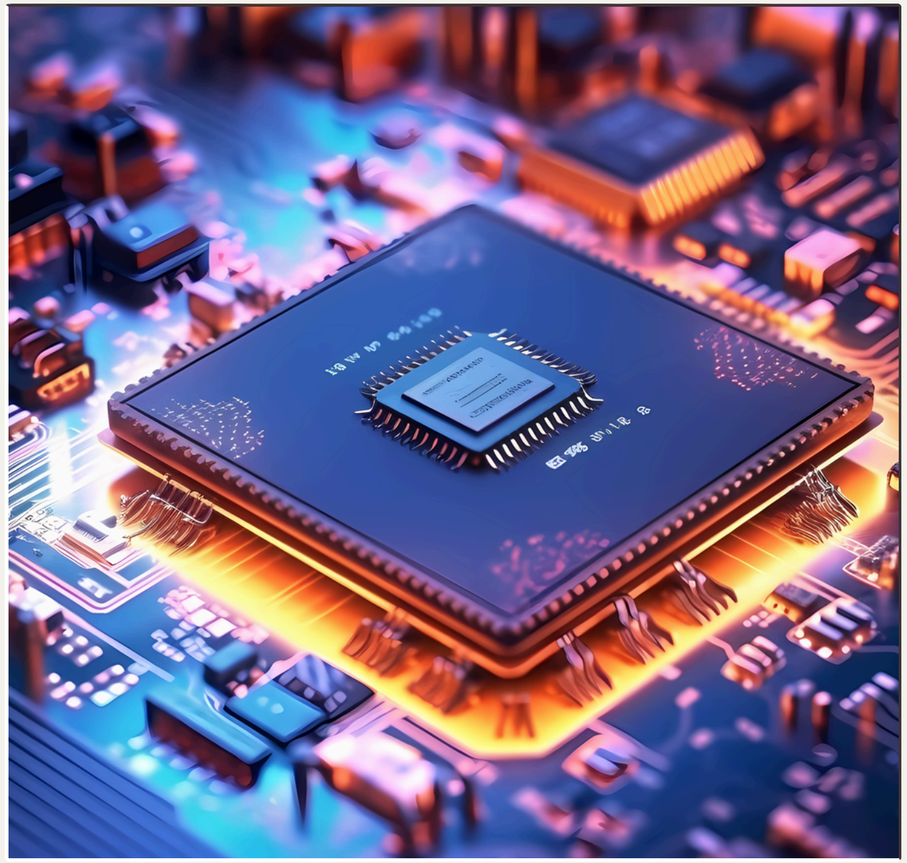


Preparing for 2026 and Beyond

The Quantum Threat

Future quantum computers will break today's encryption. Encrypted information stolen today can be decrypted in the future.

Begin assessing which data requires long-term confidentiality and start planning your transition to post-quantum cryptography.



Don't wait for a crisis. Make digital security a strategic priority today

''In a digital world, your mission cannot survive without cybersecurity. By acting today, you do more than def end systems. You defend trust."

the presentation is over

Ali Selim KARA
Communication Specialist and Youth Trainer

aliselimkara@gmail.com
/aliselimkara