What is cyber security?

the practice

Cybersecurity is the practice of protecting computers, networks, and digital information from theft, damage, or unauthorized access by hackers and malicious software

- CIA Triad

1. Confidentiality is all about keeping sensitive information private. Only people who are supposed to see it should be able to, and that's where a strong authentication process like multi-factor authentication comes into play.

2. Integrity means being able to trust your data. It shouldn't be altered without permission; you need to know it's accurate and complete. Businesses use tools like digital signatures, backup systems, and version control to ensure critical information, from invoices to patient records, stays exactly the way it should.

3. Just as unauthorized users must be kept out of an organization's data, data should be available to legitimate users whenever required. This means keeping systems, networks, and devices up and running.

- Real examples

Confidentiality breach

A healthcare staffing platform, ESHYFT, exposed over 86,000 records, complete with social security numbers, professional credentials, and scanned IDs, in a publicly accessible Amazon S3 bucket for months. There was no encryption or access control, and security researchers disclosed the exposure before the firm secured its cloud assets

Integrity violation

Financial systems often pause file integrity checks during maintenance windows. One organization discovered that attackers had retroactively edited transaction logs on a billing system to hide fraudulent transfers. With integrity monitoring disabled during a patch cycle, the manipulation went undetected until discrepancies surfaced during reconciliation.

Availability failure

In London, hospitals served by Synnovis, a diagnostic laboratory for major NHS trusts, experienced significant disruptions after a ransomware attack shut down their IT systems. Over 1,500 surgical procedures and outpatient services were postponed. Systems remained offline for days, and clinical capacity dropped sharply.

Types of attackers

1. Script Kiddies

Script kiddies are **inexperienced attackers** who use **ready-made tools and scripts** available online. They mainly attack poorly secured systems.

Common attacks:

- Website defacement
- Basic DDoS attacks
- Brute-force logins

2. Insider Threats

Insiders are **employees or contractors** with authorized access who misuse it either **intentionally or accidentally**.

Common attacks:

- Data leakage
- Credential misuse
- Policy violations

3. Hacktivists

Hacktivists attack systems to support **political or social causes**. Their goal is usually **public attention**, not money.

Common attacks:

- Website defacement
- Data leaks
- DDoS campaigns

---

4. Nation-State Actors

Nation-state actors are **government-backed hackers** with advanced skills, also known as **Advanced Persistent Threats (APTs)**.

Common attacks:

- Cyber espionage
- Zero-day exploitation
- Critical infrastructure attacks

Attack Surface

The attack surface is the number of all possible points, or attack vectors, where an unauthorized user can access a system and extract data. The smaller the attack surface, the easier it is to protect.

1. Web Applications 🌐

Web applications are one of the **most targeted attack surfaces** because they are publicly accessible.

Common vulnerabilities:

- SQL Injection
- Cross-Site Scripting (XSS)
- Cross-Site Request Forgery (CSRF)

Why targeted:
Poor input validation and insecure authentication.

2. Mobile Applications

Mobile apps often store sensitive data and communicate with backend servers.

Common vulnerabilities:

- Insecure data storage
- Weak authentication
- Insecure API communication

Why targeted:
Users connect over public Wi-Fi and outdated devices.

3. APIs 🔗

APIs act as the **bridge** between applications and services.

Common vulnerabilities:

- Broken authentication
- Excessive data exposure
- Improper rate limiting

Why targeted:
APIs are often exposed without proper security checks.

4. Network Infrastructure 🌐

Networks include routers, switches, firewalls, and communication channels.

Common vulnerabilities:

- Open ports
- Weak firewall rules
- Unpatched devices

Why targeted:
Misconfigurations allow attackers lateral movement.

5. Cloud Infrastructure ☁️

Cloud platforms host data, applications, and services at scale.

Common vulnerabilities:

- Misconfigured storage buckets
- Excessive permissions (IAM issues)
- Insecure cloud APIs

Why targeted:
Shared responsibility model is often misunderstood

1. Email Applications (Gmail, Outlook) 📧

Attack Surfaces:

- Web application interface
- Email attachments & links
- Authentication (passwords, OTPs)
- Mail servers & APIs

Possible Attacks:

- Phishing and spear-phishing

- Malware via attachments
- Account takeover

2. WhatsApp / Messaging Apps 💬

Attack Surfaces:

- Mobile application
- APIs and backend servers
- Media file handling
- Network communication

Possible Attacks:

- Malicious media files
- Account hijacking
- Social engineering scams

3. Banking & Payment Apps (GPay, PhonePay, Net Banking) 💳

Attack Surfaces:

- Mobile application
- Backend APIs
- Authentication systems
- Cloud infrastructure

Possible Attacks:

- Credential theft
- Man-in-the-Middle (MITM) attacks
- Fraudulent transaction