Cybersecurity

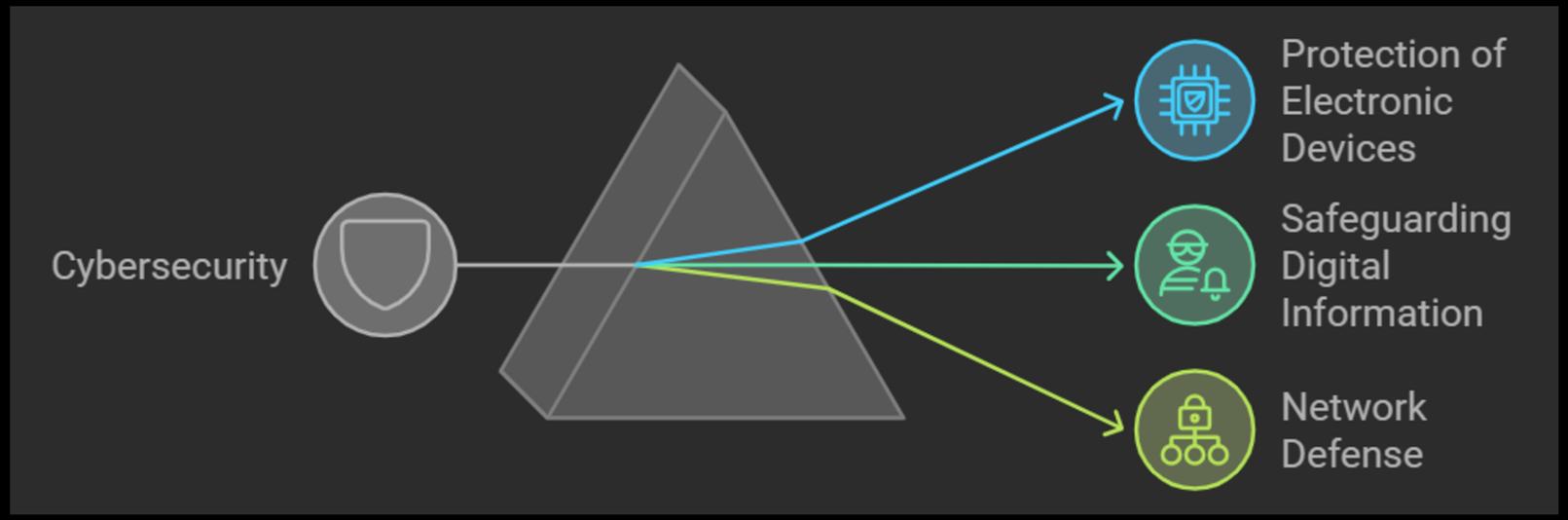
By : Hamza & achraf

1. Introduction to Cybersecurity

- Definition of Cybersecurity.
- Importance of Cybersecurity in the Digital Era.
- A Brief History of Cybersecurity.

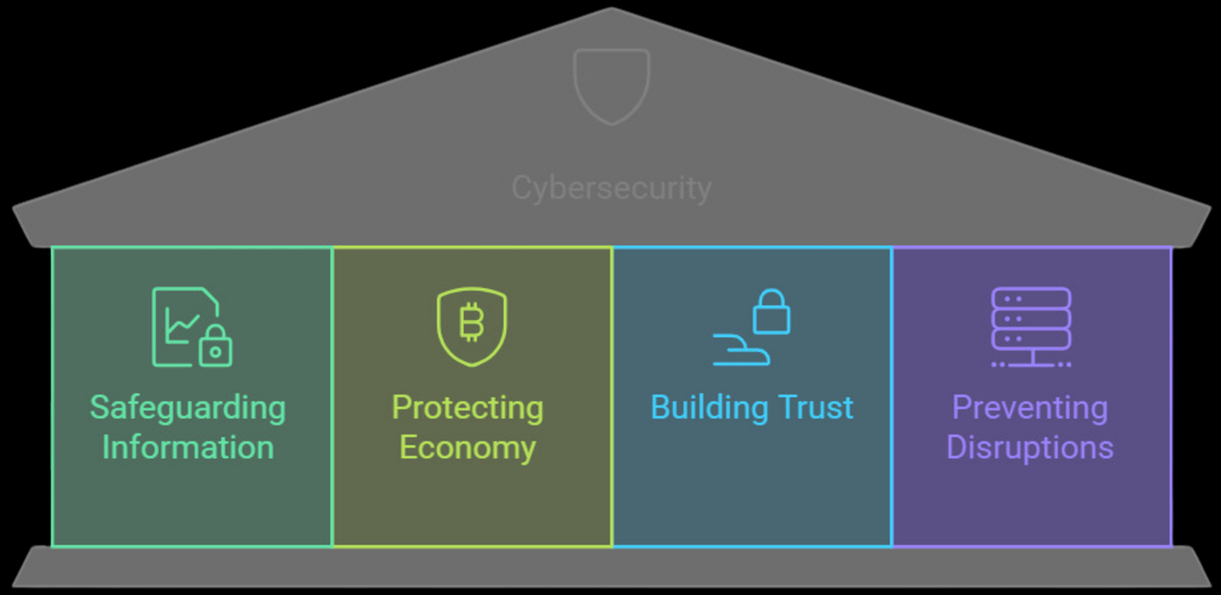
- Definition of Cybersecurity.

  Cybersecurity refers to the practice of protecting systems, networks, and software from digital attacks. These attacks aim to access, alter, or destroy sensitive information, disrupt operations, or steal data.



- # Importance of Cybersecurity in the Digital Era.

  With the increasing reliance on digital systems, cybersecurity has become a critical part of modern life.



A Brief History of Cybersecurity.

1970s:

- Cybersecurity was in its infancy and mainly focused on protecting simple databases.
- The first recorded computer virus, "Creeper", appeared in 1971 and targeted ARPANET, the predecessor of the modern internet.

1980s:

- Viruses became more sophisticated, and the first malicious software programs emerged.
- The first antivirus software was developed to counter these threats.

1990s:

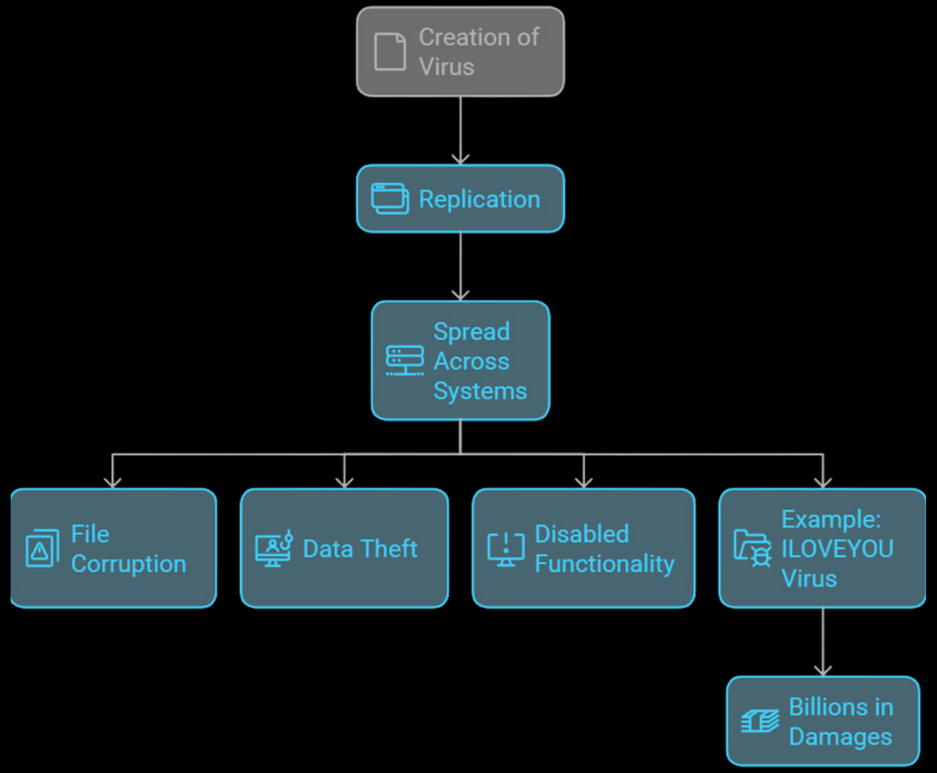
- The rise of the internet introduced new challenges, such as phishing and network-based attacks.
- Companies like Symantec were established, focusing on cybersecurity solutions.

2000s to Present:

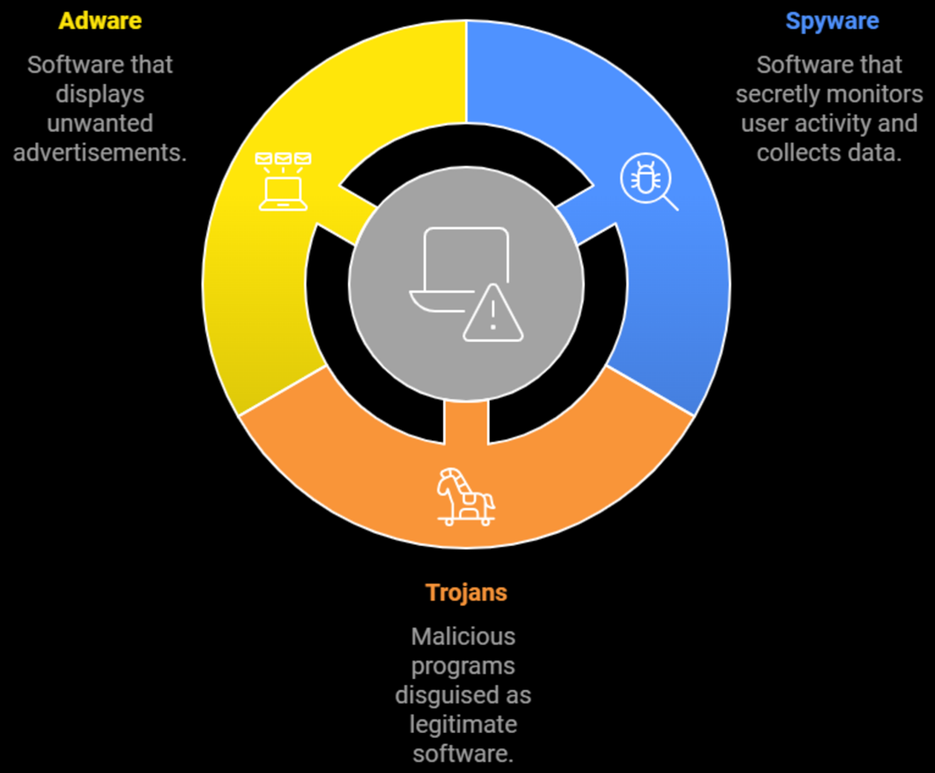
- Cyberattacks grew in scale and complexity, including ransomware and targeted attacks.
- Governments and organizations began prioritizing cybersecurity due to the increasing frequency of large-scale breaches.
- Laws and regulations, such as the General Data Protection Regulation (GDPR) in the EU, were enacted to enforce data protection.

2. Types of Cyber Threats

- Viruses

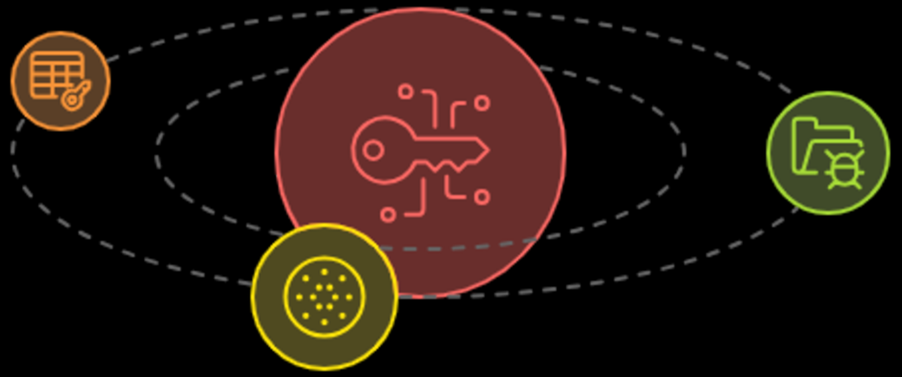


- Malware



2. Types of Cyber Threats

- Ransomware



Mechanism

Locks users out or encrypts data

Targets

Affects individuals and organizations

Example

WannaCry attack in 2017

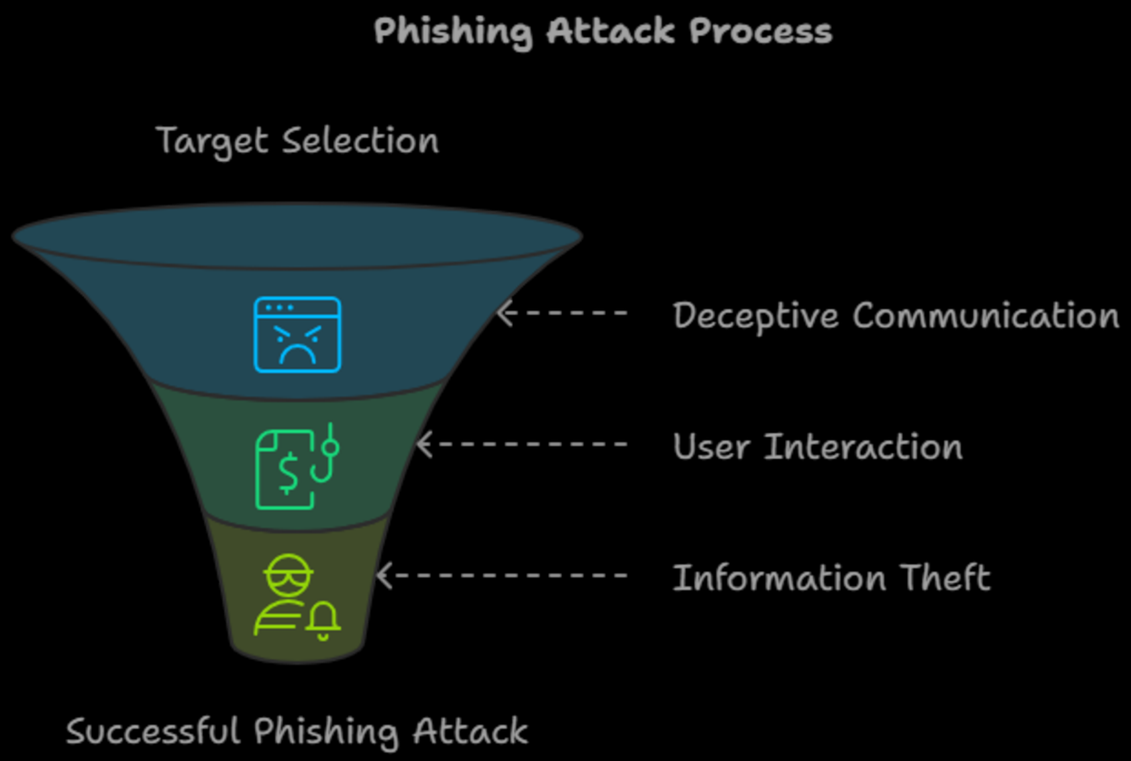
2. Types of Cyber Threats

- Phishing

  A deceptive technique where attackers pose as legitimate entities to steal sensitive information.

  Typically done through fraudulent emails, websites, or messages.

  Example: Emails pretending to be from banks requesting login credentials.

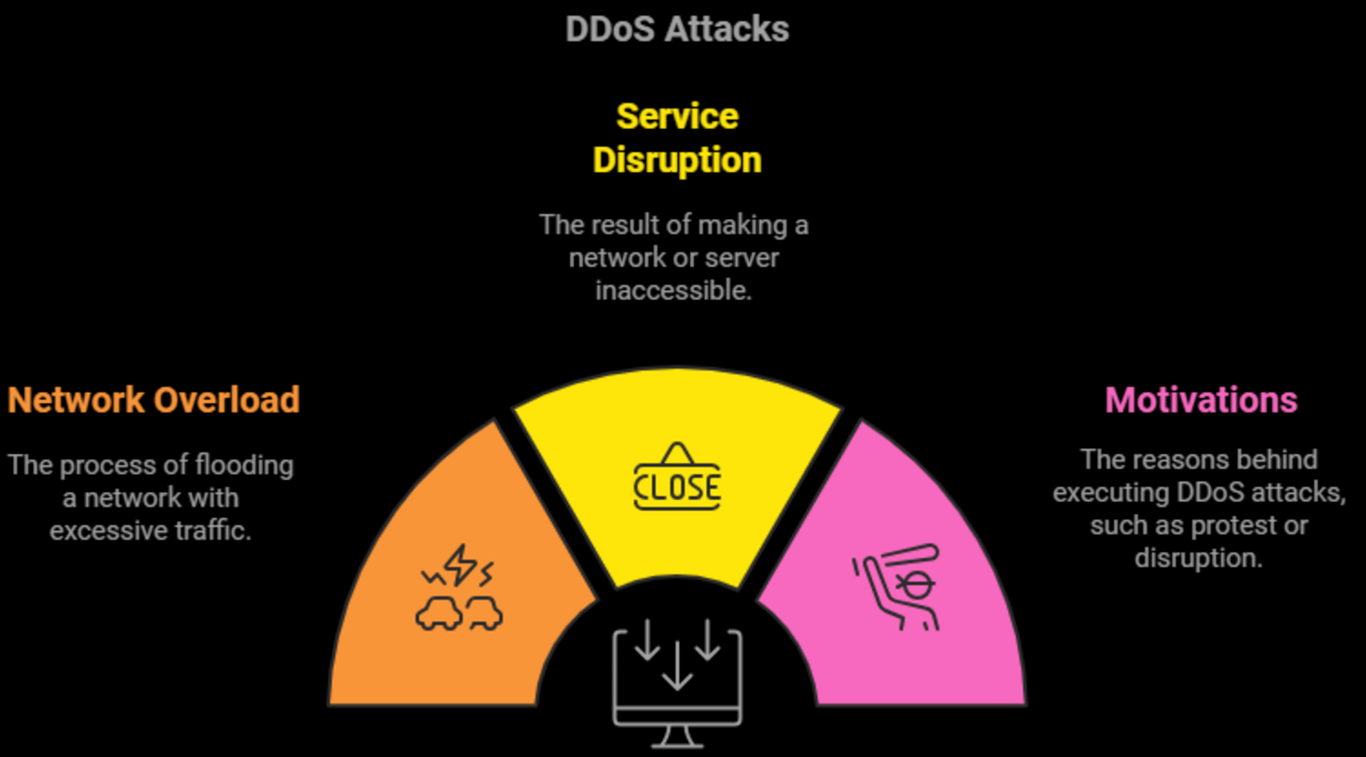


2. Types of Cyber Threats

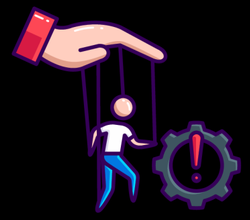
- Distributed Denial of Service (DDoS) Attacks

  Overloads a network or server with excessive traffic, rendering it inaccessible.

  Often used to disrupt business operations or protest against organizations.



3. Advanced Types of Cyber Threats



Social Engineering

- Manipulating individuals into revealing confidential information.
- Exploits human psychology rather than technical vulnerabilities.
- Example: An attacker pretending to be tech support to obtain passwords.

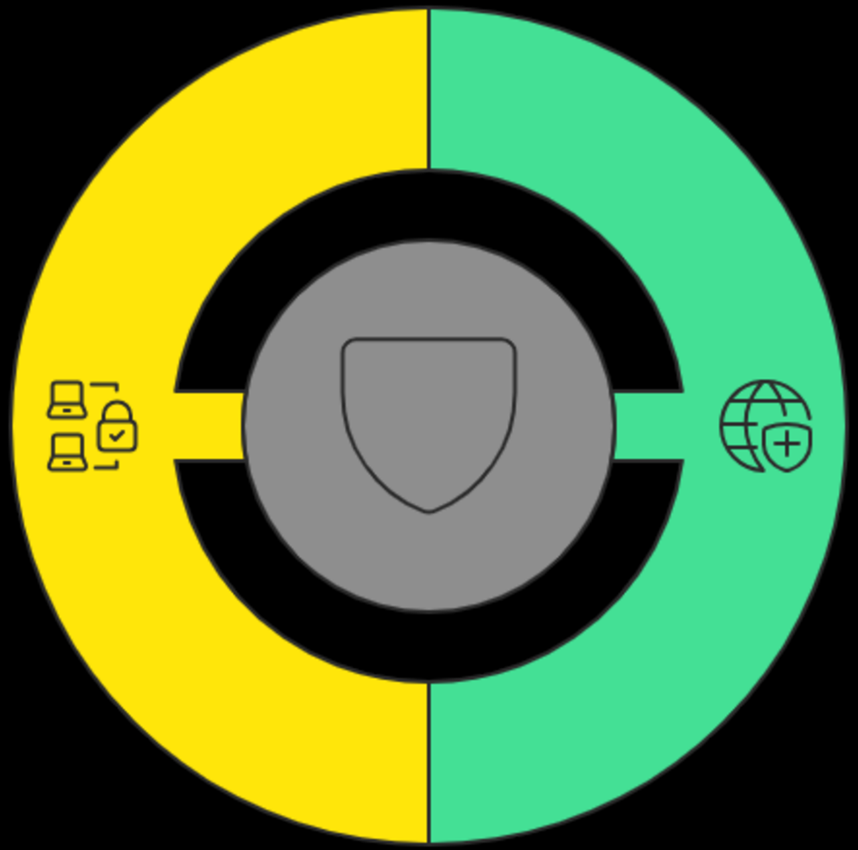
Zero-Day Attacks

- Exploits vulnerabilities in software or systems that are unknown to the vendor or public.
- Highly dangerous as there are no patches or defenses available at the time of the attack.
- Example: Zero-day vulnerabilities in Stuxnet (2010)
- SolarWinds Hack (2020)

4. Cybersecurity Defense Strategies

Personal Security Practices

Strong Passwords, Updates, Safe Browsing



Technologies

Firewalls, Antivirus Software, Encryption

5. Famous Cybersecurity Breaches

- ## Yahoo Data Breach (2013-2014)

  Yahoo suffered one of the largest data breaches in history, exposing over 3 billion accounts.

  ### How it Happened ?

  Hackers exploited weak encryption to access user data, including email addresses, passwords, and security questions.

  ### impact

  Massive reputational damage.

  Reduced Yahoo's acquisition price by Verizon by $350 million.

- ## Sony Pictures Hack (2014)

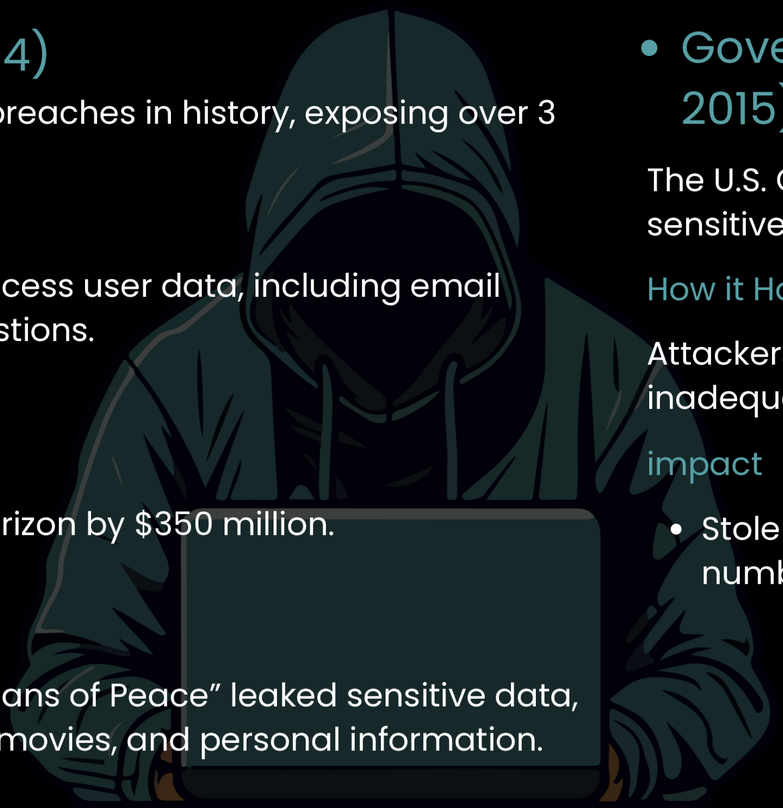
  A cyberattack by a group called “Guardians of Peace” leaked sensitive data, including employee emails, unreleased movies, and personal information.

  ### How it Happened ?

  Spear-phishing emails tricked employees into downloading malware, compromising internal networks.

  ### impact

  - Major operational disruptions.
  - Public embarrassment due to leaked emails.



- ## Government Institutions (e.g., OPM Breach, 2015)

  The U.S. Office of Personnel Management (OPM) breach exposed sensitive data of 22 million federal employees.

  ### How it Happened ?

  Attackers exploited unpatched software vulnerabilities and inadequate access controls.

  ### impact

  - Stolen data included security clearance files, Social Security numbers, and fingerprints.

6. Building a Career in Cybersecurity

Cybersecurity is one of the fastest-growing fields, offering diverse opportunities and high demand for skilled professionals. To build a successful career in cybersecurity, understanding key roles, certifications, and required skills is essential.

Key Roles in Cybersecurity

The field of cybersecurity offers a variety of roles, each catering to different interests and skill sets. Here are some of the most prominent roles:

1. Threat Analyst

A threat analyst monitors, detects, and analyzes potential cyber threats to prevent security breaches.

- Responsibilities

- Monitoring systems for unusual activity.
- Conducting risk assessments and vulnerability analysis.
- Reporting on emerging threats.

- Skills Needed:

- Knowledge of malware, phishing, and DDoS attacks.
- Proficiency in monitoring tools like Splunk or Wireshark.

2. Threat Analyst

Penetration testers simulate cyberattacks to identify vulnerabilities in a system before malicious actors exploit them.

6. Building a Career in Cybersecurity

- Responsibilities:

- Conducting simulated attacks on applications, networks, and devices.
- Documenting vulnerabilities and suggesting security measures.

- Skills Needed:

- Advanced knowledge of hacking techniques and tools.
- Strong programming skills in languages like Python and C.

3.Risk Manager:

Risk managers focus on assessing and mitigating cybersecurity risks within an organization.

Responsibilities

- Identifying security risks and vulnerabilities.
- Creating strategies to mitigate risks.
- Ensuring compliance with industry standards and regulations.

- Skills Needed:

  - Expertise in risk assessment frameworks like NIST or ISO 27001.
  - Strong understanding of business processes and policies.

6. Building a Career in Cybersecurity

1. Certifications in Cybersecurity

Certifications validate your knowledge and skills in specific areas of cybersecurity. Some of the most recognized certifications include:

- CEH (Certified Ethical Hacker):
- Focused on penetration testing and ethical hacking, this certification is ideal for aspiring penetration testers and security analysts.
- CISSP (Certified Information Systems Security Professional):
- This is a globally recognized certification for experienced professionals who want to advance into roles like security manager or consultant.
- CompTIA Security+:
- A beginner-friendly certification that covers the fundamentals of cybersecurity.

Thank you all for listening