15 Common Types of Cyber Attacks

01 Social Engineering

- **What it is:** A manipulation technique where attackers trick individuals into revealing confidential information, often through deceptive emails or messages.
- **What it includes:** Phishing emails, fake websites, and phone calls pretending to be legitimate organizations.
- **Risks:** Identity theft, data breaches, and malware infections.
- **Mitigation:** Educate users about common scams, use email filters, and implement multi-factor authentication (MFA).

02 Phishing

- **What it is:** Fraudulent attempts to steal your personal information by pretending to be a trustworthy source.
- **What it includes:** Fake emails, websites, or messages that appear to come from legitimate organizations.
- **Risks:** Identity theft, unauthorized account access, and malware infection.
- **Mitigation:** Be cautious of unknown emails or links, verify sources, and use multi-factor authentication (MFA).

03 Password Attacks

- **What it is:** Attempts to crack or guess passwords to gain unauthorized access to systems.
- **What it includes:** Brute-force attacks, dictionary attacks, and credential stuffing (using stolen credentials from other breaches).
- **Risks:** Unauthorized access, data breaches, and identity theft.
- **Mitigation:** Use strong, unique passwords, enable multi-factor authentication, and employ account lockout mechanisms after failed attempts.

04 Brute Force Attack

- **What it is:** An attack where an attacker repeatedly tries all possible combinations of passwords or encryption keys until the correct one is found.
- **What it includes:** Automated software trying thousands or millions of password combinations.
- **Risks:** Unauthorized access to accounts, data breaches, and potential control over critical systems.
- **Mitigation:** Use strong, complex passwords, enable account lockouts after multiple failed attempts, and implement MFA.

05 Malware

- **What it is:** Malicious software designed to damage or disrupt systems, steal data, or gain unauthorized access.
- **What it includes:** Viruses, Trojans, worms, spyware, and ransomware.
- **Risks:** Can steal sensitive information, corrupt data, or cause system outages.
- **Mitigation:** Use antivirus software, keep systems updated, and avoid suspicious downloads or links.

06 Ransomware

- **What it is:** A type of malware that locks or encrypts your files and demands payment (ransom) to unlock them.
- **What it includes:** Encryption of files, ransom demands, and possible data loss.
- **Risks:** Financial loss, downtime, and exposure of sensitive data.
- **Mitigation:** Regularly back up data, use strong security software, and educate employees about phishing.

07 DoS / DDoS Attacks

- **What it is:** Attacks that overwhelm a website or service with traffic, making it unavailable to users.
- **What it includes:** Flooding a network with data to exhaust resources.
- **Risks:** Downtime, loss of revenue, and reputation damage.
- **Mitigation:** Use DDoS protection services, network redundancy, and rate limiting.

08 Session Hijacking

- **What it is:** An attack where an attacker takes control of a user's active session, typically by stealing session cookies or tokens.
- **What it includes:** Intercepting or stealing session IDs to gain unauthorized access to a user's active session without their knowledge.
- **Risks:** Unauthorized access to accounts, data theft, and fraud.
- **Mitigation:** Use secure cookies (with the HttpOnly and Secure flags), encrypt sessions, and ensure secure connections (HTTPS).

9 Man-in-the-Middle (MITM) Attack

- **What it is:** An attack where an attacker intercepts and alters communication between two parties.
- **What it includes:** Stealing login credentials, injecting malicious content into communications.
- **Risks:** Data theft, fraud, and privacy breaches.
- **Mitigation:** Use encryption (HTTPS), avoid public Wi-Fi for sensitive transactions, and implement secure communication protocols.

10 SQL Injection

- **What it is:** A type of attack where malicious code is inserted into a website's database through input fields to manipulate data.
- **What it includes:** Unauthorized access, deletion, or modification of database records.
- **Risks:** Data breach, unauthorized data access, and financial loss.
- **Mitigation:** Implement input validation, use prepared statements, and regularly test for vulnerabilities.

11 Insider Threats

- **What it is:** Threats that come from within the organization, often by employees or trusted individuals.
- **What it includes:** Data theft, sabotage, or negligence leading to security breaches.
- **Risks:** Intellectual property theft, loss of trust, and financial losses.
- **Mitigation:** Monitor user activity, enforce least-privilege access, and educate employees about security policies.

12 Cross-Site Scripting (XSS)

- **What it is:** A web attack where an attacker injects malicious scripts into a website, which then executes on users' browsers.
- **What it includes:** Data theft (e.g., session cookies), redirection to malicious websites, or defacing websites.
- **Risks:** Account compromise, theft of sensitive data, and user redirection to harmful sites.
- **Mitigation:** Validate and sanitize user input, use Content Security Policy (CSP), and implement proper security coding practices.

13 Zero-Day Exploit

- **What it is:** Attacks that take advantage of unknown vulnerabilities in software or hardware, before the developer has a chance to fix them.
- **What it includes:** Exploiting software bugs or unpatched vulnerabilities.
- **Risks:** Significant damage, as there's no immediate fix or defense available.
- **Mitigation:** Keep software updated, use security patches promptly, and use threat intelligence to detect unusual behavior.

14 Supply Chain Attacks

- **What it is:** An attack that targets weaknesses in an organization's supply chain, often compromising software or hardware before it reaches the target.
- **What it includes:** Malware inserted into software updates or hardware components during manufacturing or distribution.
- **Risks:** Data breaches, long-term security vulnerabilities, and compromised business operations.
- **Mitigation:** Vet suppliers, use trusted software and hardware sources, and implement software integrity checks.

15 AI-Powered Attacks

- **What it is:** Cyberattacks that use artificial intelligence to automate and enhance the efficiency of attack strategies.
- **What it includes:** AI-driven malware, spear-phishing using AI to craft more convincing messages, and AI tools to bypass security defenses.
- **Risks:** Faster and more precise attacks, evasion of traditional defenses, and increased scale of attacks.
- **Mitigation:** Implement AI-based detection systems, keep security systems updated, and use behavior analytics to spot anomalies.