Unit – 3

Understanding Cyber Threats and Vulnerabilities

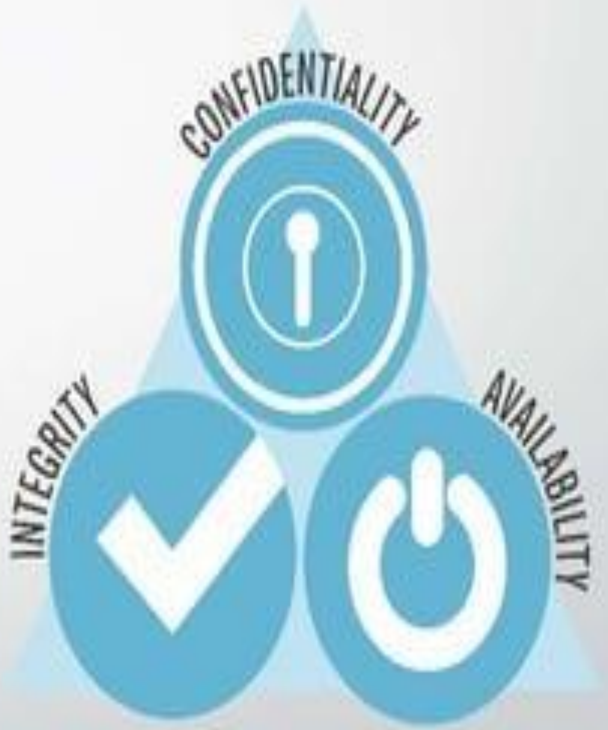
Prepared By : Jayshree Dasa

What is cyber security ?

Cybersecurity is the protection of internet-connected systems including Hardware, software and Data from cyber attacks.

❖ The key concept of cyber security ?

The cyber security on a whole is very broad term but is based on three fundamental concepts known as “**The CIA triad**”



❖ Three fundamental principal of cyber security

✓Confidentiality

✓Integrity

✓Availability

Availability:- Availability guarantees that systems, applications and data are available to users when they need them. The most common attack that impacts availability is **denial-of-service** in which the attacker interrupts access to information, system, devices or other network resources.

Integrity:- is the ability to ensure that a system and its data has not suffered unauthorized modification. Integrity protection protects not only data, but also **operating systems**, **applications** and **hardware** from being altered by **unauthorized** individuals.

Confidentiality:- ensures that data exchanged is not accessible to unauthorized users. The users could be applications, processes, other **systems** and/or **humans**

What are cyber Threats?

Cyber Threat

- A cyber threat is any potential danger that could harm your computer systems, networks, or data. It’s like a looming danger, such as a virus, hacking attempt, or phishing attack.

What are Cyber Threats?

Cyber Threats are malicious attacks that damage and steal data which in turn affects the **digital life**

Sources of Cyber Threats:-

- State-sponsored
- Terrorists
- Industrial spies
- Organized crime groups
- Hackers
- Hacktivists
- Cyber espionage

Vulnerability

- A vulnerability is a weakness in your system that could be exploited by a cyber threat. For example, outdated software or weak passwords are vulnerabilities that hackers can take advantage of.

Differentiate Between a Cyber Threat and a Vulnerability

Aspect	Cyber Threat	Vulnerability
Definition	A potential danger or event that could exploit a vulnerability to cause harm or damage.	A weakness or flaw in a system, network, or application that can be exploited by a threat
Example	Phishing attacks, malware, ransomware, DDoS attacks.	Unpatched software, weak passwords, unsecured networks.
Control	Managed through security measures like firewalls, intrusion detection systems (IDS), and anti-malware tools.	Managed through vulnerability assessments, patch management, and regular security updates.
Objective	Intent to harm, steal, or disrupt.	Unintended weakness that needs to be secured.
Detection	Identified through threat intelligence, monitoring suspicious activities.	Identified through vulnerability scanning, security audits, and testing.

Types of Cyber Threats

Types of Cyber Threats

- **Malware:** Software designed to harm or exploit systems, like viruses or worms.
- **Phishing:** Fake emails or messages designed to trick you into giving away sensitive information.
- **Denial of Service (DoS) Attacks**: Overloading a system so that it becomes unavailable to users.
- **Ransomware:** A type of malware that locks your files until you pay a ransom.
- **Spyware:** Software that secretly gathers information about you without your consent.

Types of Cyber Threats

- **Man-in-the-Middle (MitM) Attacks:** An attack where the attacker secretly intercepts and possibly alters communication between two parties.
- **SQL Injection:** An attack where malicious code is injected into a SQL query to manipulate a database

Case Study Summary: SolarWinds Cyber Attack

Background: In December 2020, a major cyber attack was discovered targeting the SolarWinds Orion software, used by thousands of organizations worldwide, including U.S. government agencies and Fortune 500 companies. The attack was attributed to a state-sponsored group believed to be associated with a foreign government.

Cont….

Nature of the Attack: The attackers gained unauthorized access by compromising the SolarWinds software update process. They inserted a malicious code, known as "Sunburst," into a legitimate software update released by SolarWinds. When customers installed the update, the malware created a backdoor to their systems, allowing the attackers to infiltrate networks, steal sensitive data, and monitor communications.

Cont….

Impact: The breach affected over 18,000 organizations globally, including critical sectors such as government, finance, healthcare, and energy. High-profile agencies like the U.S. Department of Treasury, Department of Homeland Security, and parts of the Pentagon were compromised. The attack revealed the vulnerabilities of supply chain security and the sophisticated nature of state-sponsored cyber operations.

Cont….

Strengthening Supply Chain Security: Organizations must scrutinize third-party software and updates to prevent similar attacks.

Improving Detection Capabilities: Enhanced monitoring and detection tools can help identify unusual activity sooner.

Collaboration and Information Sharing: International cooperation is vital to respond effectively to state-sponsored cyber threats and to develop coordinated defense strategies.

Reference

https://www.ibm.com/docs/en/randori?topic=2022-solarwinds-orion-cve-2020-10148

Types of cyber Threats

- Phishing attack
- SQL Injection threat
- Man-in-the-middle attack
- Malware
- Zero-day attack
- Cross-site-scripting
- Advanced persistent threats
- Password attack

Phishing Attack

Phishing is the technique to steal a user's data from the **internet** or **computer-connected device**.

Types of Phishing attacks

- Phishing email
- Domain spoofing
- Voice phishing
- SMS phishing
- Clone phishing
- Typo squatting
- Evil twin
- Whale phishing

Ways to prevent Phishing attack

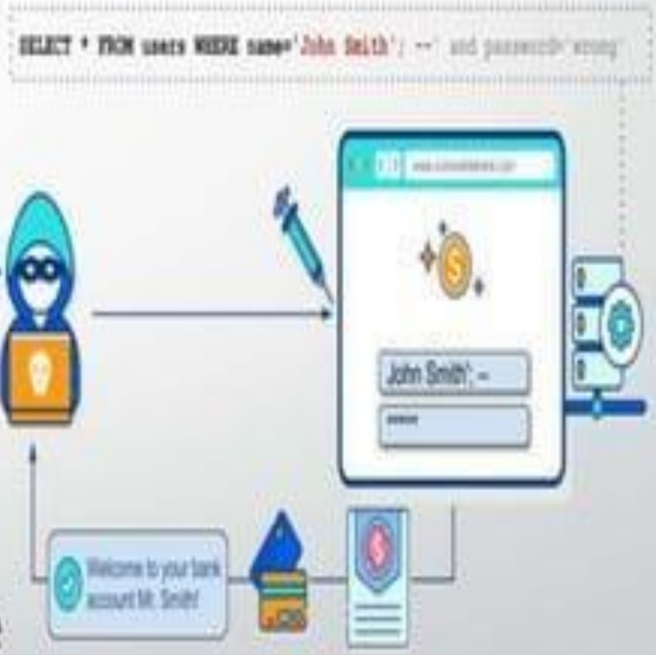
- Know what a phishing scam looks like
- Don't click on a random **link**
- Get free **anti-phishing** add-ons
- Don't give your information to an unsecured site
- Change **passwords** regularly
- install **firewall**

SQL injection threat

In the SQL injection threat, the attacker sends a malicious query to the device or a server. The server is then forced to expose sensitive information.

Ways to prevent SQL injection threat:-

- Validate user inputs
- **Sanitize** data by limiting special characters
- Use stored procedures in the **database**
- Establish appropriate **privileges** and **strict**



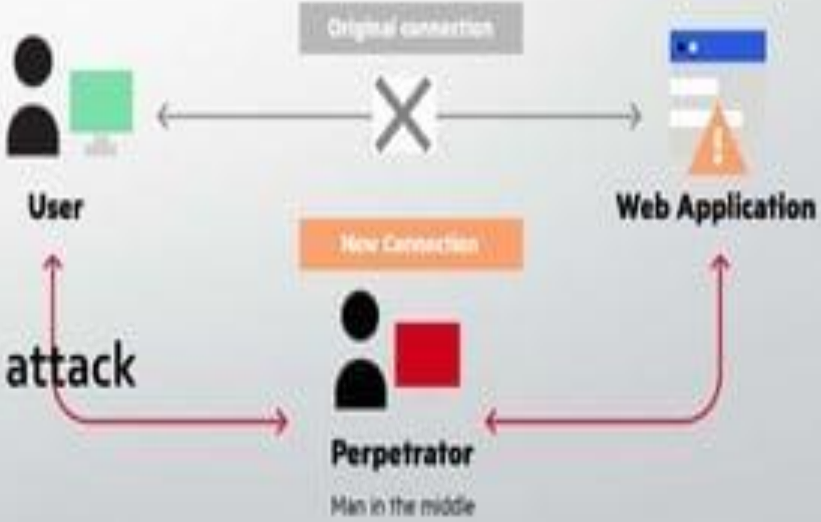
```
SELECT * FROM users WHERE name='John Smith'; --' and password='wrong'
```

Man-in-the-middle attack

The man-in-the-middle attack is a security breach where cybercriminals place themselves between the **communication system** of a **client** and the **server**.

Types of Man-in-the-middle attack

- Session hijacking
- IP spoofing
- Replay



Ways to prevent Man-in-the-middle attack

- Strong router login credentials
- Virtual private network
- Strong encryption on access points
- Force HTTPS Man-in-the-middle attack P

Cont…

Session Hijacking : It's a form of attack where a bad actor steals or manipulates the session token to gain unauthorized access to information or services.

IP spoofing : An IP spoofing attack is a cyber attack where an attacker creates fake IP packets to impersonate a computer system and carry out malicious actions. IP spoofing is difficult to detect because it's carried out at the network level, and spoofed connection requests can appear legitimate.

Replay Attack : Replay attacks are a form of network attack where an attacker intercepts and retransmits data that was previously exchanged between two parties.

Malware

Malware is a malicious software which gets installed into the system when the user clicks on a dangerous **link** or an **email**.

What Is Malware
Rootkits
Spyware
Ransomware
Worms
Remote Access
Virus
Keylogger
educba.com

Types of Malware:-

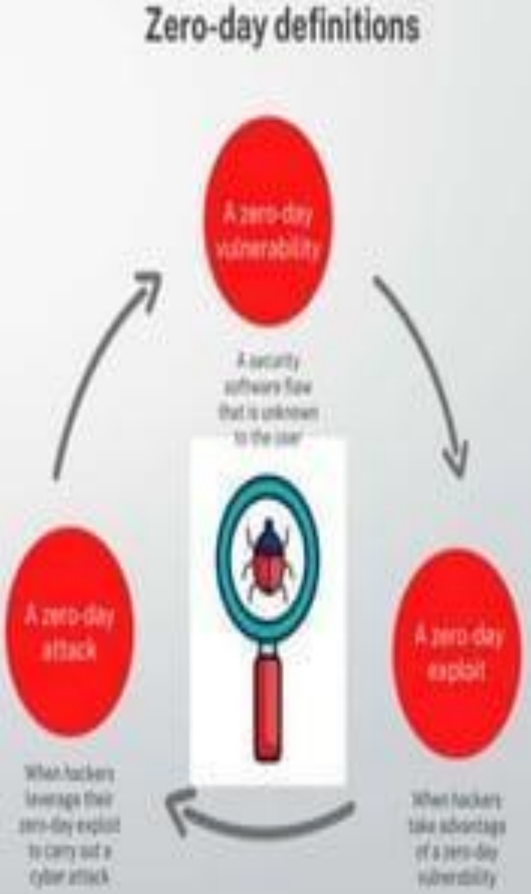
- Viruses
- Trojans
- Worms
- Ransomware

Ways to prevent Malware:-

- Regularly update your computer and software
- Be careful while opening unknown email attachments or images

Zero-day-Attack

A zero-day attack is an attack done by hackers when the network, hardware or software **vulnerability** is **announced publicly**.

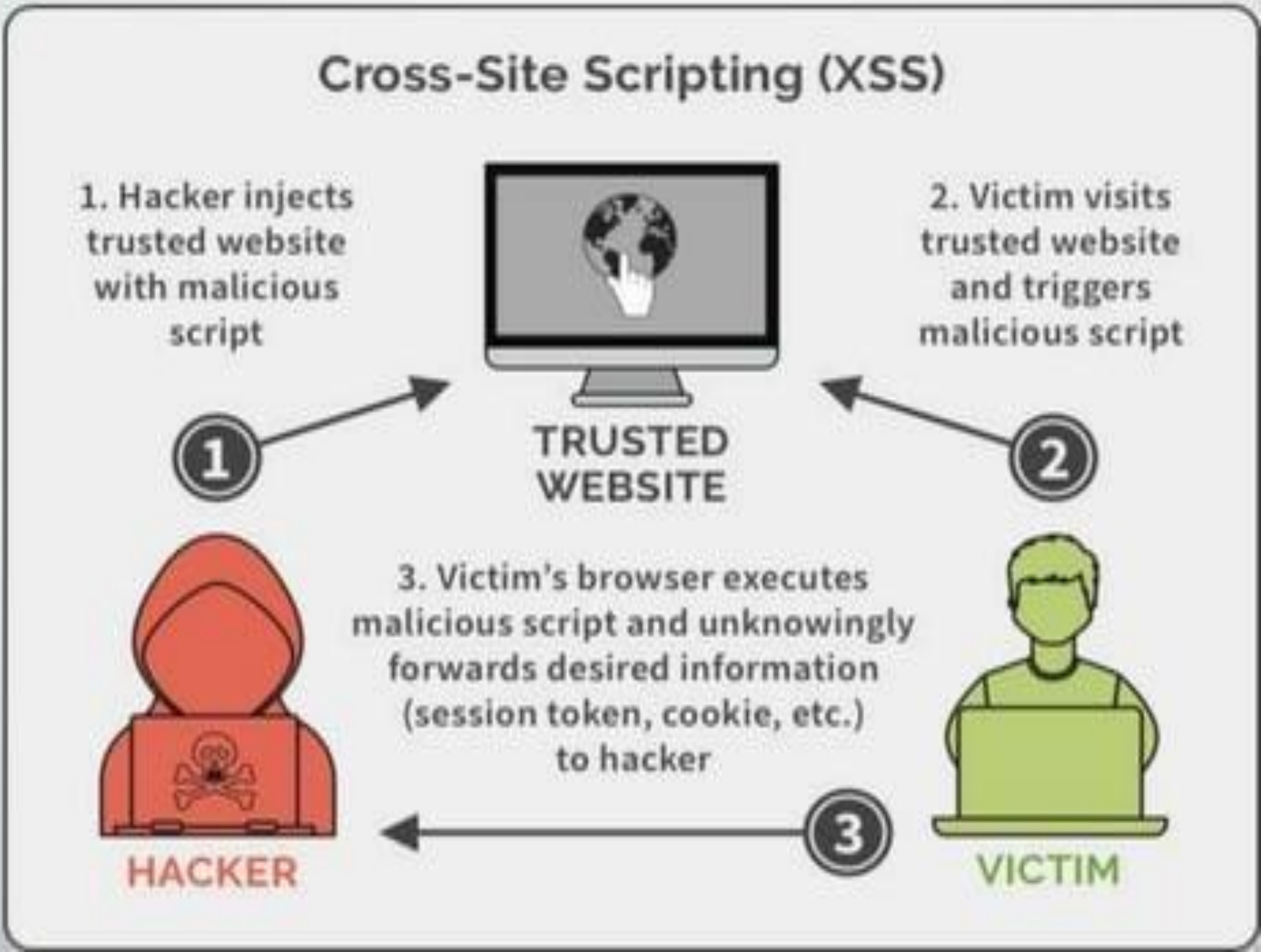

Zero-day definitions
A zero-day vulnerability
A security software flaw that is unknown to the user
A zero-day exploit
When hackers take advantage of a zero-day vulnerability
A zero-day attack
When hackers leverage their zero-day exploit to carry out a cyber attack

Ways to prevent Zero-day Attack :-

- Use an advanced, proactive email security solution
- Educate users
- Deploy a web application firewall
- Implement network access control Zero-day attack

Cross-site scripting

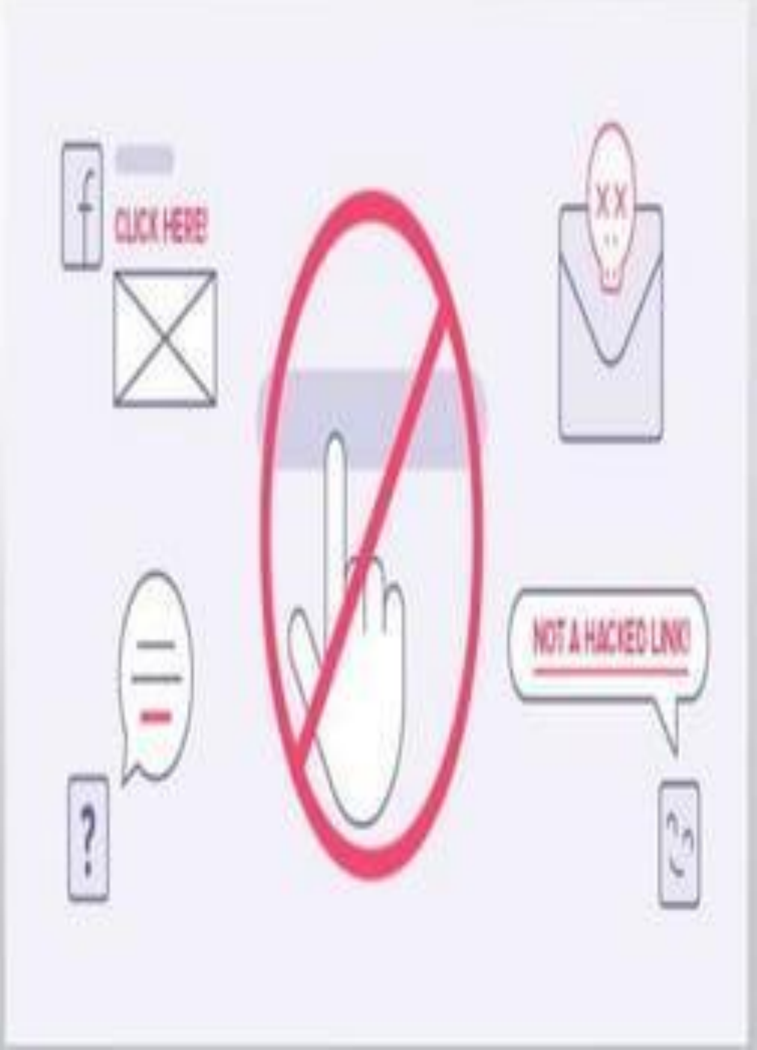
Cross-site scripting is a cyber-attack where an attacker sends **malicious code** to a reputable website


Cross-Site Scripting (XSS)
1. Hacker injects trusted website with malicious script
2. Victim visits trusted website and triggers malicious script
1
2
TRUSTED WEBSITE
3. Victim's browser executes malicious script and unknowingly forwards desired information (session token, cookie, etc.) to hacker
3
HACKER
VICTIM

Cross-site scripting

Ways to prevent Cross-site-scripting:-

- Filter input on arrival.
- Encode data on output.
- Use appropriate response headers.
- Content security policy.



Advanced persistent threat

An advanced persistent threat occurs when an attacker gains **unauthorized access** to a system or network and remains **undetected** for a **long duration**.

Ways to prevent Advanced persistent threats:-

- Install a firewall
- Enable a web application firewall
- Install an antivirus
- Implement intrusion prevention systems
- Create a sandboxing environment
- Install a VPN

Password attacks

Password attack is an attempt to **steal** passwords from a user.

Two common techniques used to get user's password :-

- Brute-force guessing
- Dictionary attack Ways to prevent Password attack
- Use strong password
- Multi-factor authentication

Analyze Types of Current Cyber Threats

- **Advanced Persistent Threats (APTs):** Lis a long-term and targeted cyber attack. It is usually carried out by highly skilled hackers, often sponsored by a state or an organized group, aiming to steal sensitive information, spy on organizations, or disrupt operations.
- **Zero-Day Exploits:** is a type of cyber attack that takes advantage of a security flaw or vulnerability in software or hardware that the manufacturer or developers do not yet know about. Because there is "zero days" of warning, no patch or fix is available to protect against the exploit.

Analyze Types of Current Cyber Threats

- **Cryptojacking:** Unauthorized use of someone’s computer to mine cryptocurrency.is a type of cyber attack where hackers secretly use your computer’s resources to mine cryptocurrency without your permission. Mining cryptocurrency involves solving complex mathematical problems to validate transactions on a blockchain network, which requires a lot of computing power.
- **Insider Threats:** Threats that originate from within the organization, often by employees who misuse their access.

Current Cyber Threats

- **Ransomware Attacks:** Increasingly common, where attackers demand money to unlock your data.
- **Phishing Campaigns:** More sophisticated attempts to steal personal or financial information.
- **Social Engineering:** Tricking people into revealing confidential information by pretending to be someone trustworthy.

Concept of Malware and Techniques to Guard Against It

- **Malware:** Malicious software designed to harm your computer or steal your data. Common types include viruses, worms, and Trojans.
- **Protection Techniques:**
  - **Use Antivirus Software:** Regularly scan your system for malware.
  - **Keep Software Updated**: Apply security patches to close vulnerabilities.
  - **Avoid Suspicious Links:** Don’t click on links or download attachments from unknown sources.

Cont.….

- **Install and Update Anti-Malware Software:** Regularly update and run anti-malware programs to detect and remove malicious software.
- **Regular Software Updates:** Keep software, operating systems, and applications up-to-date to patch vulnerabilities.
- **Use of Firewalls:** Implement firewalls to block unauthorized access to systems.
- **Regular Backups:** Perform regular backups to restore data in case of a malware attack.
- **Educate Users:** Train employees and users on safe online practices, such as not downloading untrusted software.

Perpetrators of Malicious Hacking

- **Hackers:** Individuals who gain unauthorized access to systems, sometimes for malicious purposes.
- **Cybercriminals:** Professional criminals who use hacking to make money, often through theft or fraud.
- **Hacktivists:** Hackers with a political or social agenda, often targeting organizations they disagree with.

Characteristics of Vulnerabilities

- **Weaknesses in Software:** Bugs or flaws in software that can be exploited.
- **Poor Security Practices:** Such as weak passwords, unencrypted data, or lack of updates.
- **Human Error:** Mistakes made by users, like clicking on phishing links or not updating software.

Prevention of and Protection Against Cyber Threats

- **Regular Updates:** Keep your software and systems up to date.
- **Strong Passwords:** Use complex passwords and change them regularly.
- **Use Firewalls:** Protect your network from unauthorized access.
- **Educate Users:** Teach employees or users about safe online practices, such as recognizing phishing attempts.
- **Backup Data:** Regularly back up important data to minimize damage in case of an attack.

Cont.….

- **Regular Security Audits:** Conduct thorough audits to identify and address vulnerabilities.
- **Access Control:** Implement strict access controls to ensure that only authorized individuals have access to critical systems.
- **Multi-Factor Authentication (MFA):** Use MFA to add an extra layer of security to user logins.
- **Encryption:** Encrypt sensitive data to protect it from unauthorized access during transmission and storage.
- **Incident Response Plan:** Develop and maintain an incident response plan to quickly address and mitigate the impact of security breaches.
- **Employee Training:** Regularly train employees on security best practices, including recognizing phishing attempts and handling sensitive information securely.

Thank you