**Cyber Attacks**

**Phishing**

**Phishing** is the fraudulent attempt to obtain sensitive information such as usernames, passwords, and credit card details by disguising oneself as a trustworthy entity in an electronic communication. Typically carried out by email spoofing or instant messaging, it often directs users to enter personal information at a fake website that matches the look and feel of the legitimate site.

| **https://docs.google.com/uc?id=1h81YXIuk_5nljcPCklSONNbWh_Hgjbj2** |
| --- |
| *Phishing web site acting like Paypal's official website* |

Phishing is an example of social engineering techniques being used to deceive users. Users are often lured by communications purporting to be from trusted parties such as social web sites, auction sites, banks, online payment processors or IT administrators. The above screenshot belongs to a phishing site, not the genuine PayPal site. If you type your username and password at this fake site, your credentials will be sent to the bad guy and then he will gain access to your account.

**Q: Explain Phishing and how to prevent it.**  
A: Phishing is a Cyberattack in which a hacker disguises as a trustworthy person or business and attempt to steal sensitive financial or personal information through fraudulent email or instant message.  
You can prevent Phishing attacks by using the following practices:

* Don’t enter sensitive information in the webpages that you don’t trust
* Verify the site’s security
* Use Firewalls
* Use AntiVirus Software that has Internet Security
* Use Anti-Phishing Toolbar

**Malware**

The term **malware** is a contraction of **mal**icious soft**ware**. Put simply, malware is any piece of software that was written with the intent of damaging devices, stealing data, and generally causing a mess. Viruses, trojans, spyware, and ransomware are among the different kinds of malware.

A **computer virus** is a type of malicious code or program written to alter the way a computer operates and is designed to **spread** from one computer to another.

A Trojan horse or **Trojan** is a type of malware that is often disguised as legitimate software. Trojans can be employed by cyber-thieves and hackers trying to gain access to users' systems. Users are typically tricked by some form of social engineering into loading and executing Trojans on their systems.

**Spyware** is a type of malware that's hard to detect. It collects information about your surfing habits, browsing history, or personal information (such as credit card numbers), and often uses the Internet to pass this information along to third parties without you knowing.

**Ransomware Trojan** is a type of cyberware that is designed to extort money from a victim. Often, ransomware will demand a payment in order to undo changes that the Trojan virus has made to the victim’s computer.

| **https://docs.google.com/uc?id=1xX--vKdQJosSf4pgrhqQ1hiMH0vtF22n** |
| --- |
| *Bad guy* |

**Q: Define Spyware.**  
A: Spyware is a malware that aims to steal data about the organization or person. This malware can damage the organization's computer system.

**SQL Injection-XSS-CSRF**

**SQL injection** is a code injection technique that might destroy your database. This type of attack usually occurs when you ask a user for input, like their user-name/user-id, and instead of a name/id, the user (bad guy) gives you an SQL statement that you will unknowingly run on your database.

**Cross-Site Scripting (XSS)** attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end-user.

**Cross-site Request Forgery (CSRF)** is a very common vulnerability. It's an attack that forces a user to execute unwanted actions on a web application in which the user is currently authenticated.

| **https://docs.google.com/uc?id=1q2lyqohBacXZWaKmahdQio-Xo7CCc-YI** |
| --- |
| *Injecting SQL querry to web site form* |

**Q: Explain SQL Injection and how to prevent it.**A: SQL Injection (SQLi) is a code injection attack where an attacker manipulates the data being sent to the server to execute malicious SQL statements to control a web application’s database server, thereby accessing, modifying and deleting unauthorized data. This attack is mainly used to take over database [servers](https://lms.clarusway.com/mod/lesson/view.php?id=1015" \o "Servers).  
You can prevent SQL Injection attacks by using the following practices:

* Use prepared statements
* Use Stored Procedures
* Validate user input