**Types of Email Attacks**

 Many people depend on the Internet for professional, social, and personal activities, but there are individuals who try to damage computers and violate privacy.

 Email is a widely used service, with over a billion users globally.

 Due to its popularity, email has become a major vulnerability for both users and organizations.

### **Phishing**

 **Phishing**: A type of fraud where cybercriminals use email, instant messaging, or social media to steal information like login credentials by pretending to be a trusted source.

 **Spear Phishing**: A more targeted phishing attack where emails are customized for a specific person after researching their interests.

 **Phishing Techniques**: Cybercriminals send fake emails that appear to come from trusted sources (e.g., banks or online retailers) to trick users into sharing personal or financial details.

 **Advantage**: Phishing attacks are easy to carry out using basic social engineering tactics, requiring little technical knowledge.

* **Disadvantage**: Phishing can be easily detected if users are aware of the legitimate source of the email and are cautious about clicking links or downloading attachments.

### **Vishing**

 **Vishing**: Phishing via voice communication, where criminals spoof calls using voice-over IP technology or send recorded messages that appear legitimate to steal personal information.

 **Goal of Vishing**: Criminals aim to obtain sensitive details like credit card numbers to commit identity theft.

 **Trust Factor**: Vishing exploits people's trust in the telephone network.

 **Spear Phishing**: A targeted form of phishing where customized emails are sent to a specific individual or group, making the attack appear more legitimate.

 **Advantage of Spear Phishing**: It is highly effective because the attacker personalizes the email after researching the victim, increasing the chances of success.

### **Smishing**

 **Smishing**: Phishing via text messaging on mobile phones, where criminals impersonate a legitimate source to gain the victim's trust.

 **Attack Method**: Criminals may send a website link in a text message, leading the victim to a site that installs malware on their phone.

### **Whaling**

 **Whaling**: A type of phishing attack targeting high-profile individuals within an organization, such as senior executives, politicians, or celebrities.

 **Attack Method**: Whaling is a form of spear phishing where emails appear to come from senior executives (e.g., CEO or CFO), often requesting money transfers or sensitive information.

 **Advantage**: This attack can be highly lucrative for the attacker, potentially leading to large sums of money or valuable information.

 **Disadvantage**: Whaling requires a high level of sophistication and social engineering skills to be successful.

### **Pharming**

 **Pharming**: The act of impersonating an authorized website to deceive users into entering their credentials.

 **Attack Method**: Pharming redirects users to a fake website that looks like the official site.

### **Spyware**

 **Spyware**: Software used by criminals to track and collect information about a user's computer activities.

 **Common Features**: Includes activity trackers, keystroke logging, and data capture.

 **Security Risk**: Spyware often modifies security settings to bypass protections.

 **Distribution**: It is often bundled with legitimate software or Trojan horses, and many shareware websites host spyware

### **Scareware**

 **Scareware**: A type of software that uses fear to persuade users into taking specific actions.

 **Attack Method**: Scareware creates fake pop-up windows that look like system dialogue messages, warning that the system is at risk.

### **Spam**

 **Spam**: Unsolicited email, often used for advertising but can also contain harmful links, malware, or deceptive content.

 **Goal**: The aim is to steal sensitive information, such as social security numbers or bank account details.

## How To Protect Yourself from Email Attacks?

 Be cautious when opening emails from unknown sources.

 Look for signs of phishing, such as spelling errors, suspicious links or attachments, and requests for personal information.

 Use strong passwords and enable two-factor authentication to protect your email account.

 Keep your computer and software up-to-date with the latest security patches.

 Use antivirus and anti-malware software to detect and prevent email attacks.