PHISHING AWARENESS TRAINING

Phishing is one kind of online assault.Phishing attacks can happen through social media platforms, text messages, phone calls, or emails.Developing an online course on phishing attacks is a fantastic way to inform people about cybersecurity risks.Below are a few modules.

**Common Phishing Techniques:**

**Email Spoofing:**

**Email spoofing, which can be dangerous because it is frequently used for phishing and malware distribution, is faking the sender's address in an email to make it look like it is from a reliable source.**

**Spear Phishing: Spear phishing poses serious security risks because it targets certain people or organizations and uses tailored communications to deceive recipients into disclosing private information or taking activities.**

**Pharming:**

**Pharming is a cyberattack that compromises user security by gathering sensitive data by rerouting website traffic to fake domains, frequently via DNS cache poisoning.**

**Social Engineering:**

**Social engineering poses serious risks to security and privacy because it uses deceit, persuasion, or impersonation to trick people into disclosing private information or taking actions.**

**Spam:**

**Spam includes unwanted emails that are designed to steal money or sensitive data from their target.**

[**SEO Poisoning**](https://www.checkpoint.com/cyber-hub/cyber-security/what-is-cyber-attack/what-is-seo-poisoning/)**:**

**Some phishing attacks direct users to malicious websites by manipulating the output of common searches**

**Vishing:**

**Vishing or “voice phishing” is a phishing attack performed over the phone**

[**Smishing**](https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-phishing/what-is-smishing/)**:**

**Smishing is a phishing attack performed using SMS text messages.**

**Recognizing Phishing Emails**

**Check the Sender:**

**Verify the sender's email address for any inconsistencies or unusual domain names.**

**Look for Red Flags:**

**Watch out for generic greetings, urgent requests, grammatical errors, and suspicious attachments or links.**

**Verify Requests:**

**Be cautious of requests for sensitive information, such as passwords or financial details, especially if they seem unusual or unexpected.**

**Common phishing email tactics, such as:**

**>>Spoofed email addresses**

**>>Urgent or threatening language**

**>>Requests for sensitive information**

**>>Verify the sender's email address**

**>>Check for spelling and grammatical errors**

**>>Hover over links to reveal the true destination**

**>>Be cautious of unexpected attachments**

**Avoiding Phishing Websites:**

**Check the URL: Look for discrepancies or misspellings in the website's URL, as phishing sites often mimic legitimate domains.**

**Validate Security: Ensure that websites use HTTPS encryption and display a valid SSL certificate.**

**Use Trusted Sources: Avoid clicking on links from unsolicited emails or messages; instead, navigate directly to websites by typing the URL in the address bar.**

**>>Define phishing websites and their purpose.**

**>>Discuss how phishing websites mimic legitimate sites to deceive users.**

**>>Offer guidance on avoiding phishing websites:**

**>>Look for HTTPS encryption and a valid SSL certificate**

**>>Avoid clicking on links from unsolicited emails or messages**

**>>Type the URL directly into the browser when in doubt**

**Social Engineering Tactics:**

**Emotional Manipulation:**

**Attackers exploit emotions like fear, curiosity, or urgency to prompt immediate action.**

**Authority Impersonation:**

**Pretending to be a trusted figure, such as a company executive or IT support personnel, to gain trust.**

**Pretexting:**

**Creating a fabricated scenario to extract information or persuade individuals to take specific actions.**

**Phishing attacks are a serious threat to individuals and organizations, but with awareness and vigilance, we can mitigate the risks.Stay informed, stay cautious, and together, we can combat phishing effectively.**

**>>Define social engineering and its role in phishing attacks.**

**>>Discuss common social engineering tactics used by attackers, such as:**

**>>Emotional manipulation (e.g., creating a sense of urgency)**

**>>Authority impersonation (e.g., posing as a trusted figure)**

**>>Pretexting (e.g., fabricating a scenario to gain trust)**

**>>Provide examples and real-life scenarios to illustrate social engineering tactics.**