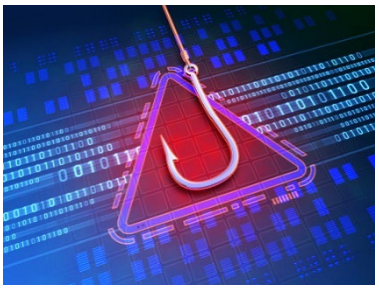
Hook, Line and Sinker - Defense Against Phishing Attacks



Phishing attacks are one of the most common methods cybercriminals use to try and gain unauthorized access to DCH's sensitive information. They are becoming increasingly sophisticated, making it more difficult for individuals to identify and avoid them. However, several measures are taken to protect DCH users against phishing attacks: user training, the PhishAlarm button, and Proofpoint email filtration.

User Training

User training is one of the most effective ways to protect against phishing attacks. Since Educating DCH users on identifying and avoiding phishing attacks is crucial in preventing successful attacks. This is achieved through online training modules, simulated phishing attacks, and in-person training sessions, which cover how to identify emails, recognize social engineering tactics, and report suspicious emails.

Simulated phishing attacks are used to test the effectiveness of user training. These simulated attacks can be sent to employees to see how many individuals fall for the phishing attempt, then this information is used to determine areas where additional training is needed.

PhishAlarm

Another effective way to defend against phishing attacks is using the PhishAlarm button. This button (which can be found in the top right corner of the DCH Outlook app) was added to allow users to report suspicious emails with a single click. The reported email is then sent to DCH's security team for further analysis and deleted from the user's inbox to prevent further interactions.

Proofpoint filtration

Proofpoint filtration can filter out phishing emails before they even reach the user's inbox. This is achieved through advanced email filtering technologies specifically designed to detect and block phishing attempts. Proofpoint filtration works by analyzing the content of incoming emails and identifying any malicious content or links. The email is then deleted or quarantined for further analysis if a phishing attempt is detected.

This method of defense is particularly effective as it blocks phishing emails before they are delivered to an inbox, helping prevent users from accidentally falling for a phishing attempt since they never even see the email.

Phishing attacks are a significant threat to DCH and its employees. If left unchecked, consequences can include identity theft, financial loss, and significant damage to the reputation of the organization. However, user training, the PhishAlarm button, and Proofpoint filtration can be effective measures to help prevent successful phishing attacks.