Cyber Security Guide

Phishing and email security

Phishing is a type of social engineering attack where an attacker attempts to trick a victim into providing sensitive information or performing an action, such as clicking on a malicious link or downloading malware. Here are some of the most common phishing techniques:

1. Deceptive phishing: This is the most common type of phishing attack. The attacker sends an email that appears to be from a legitimate source, such as a bank or an online retailer, and asks the victim to provide sensitive information, such as login credentials or credit card numbers.
2. Spear phishing: This type of attack targets a specific individual or organisation. The attacker researches the victim and creates a personalized email that appears to be from a trusted source, such as a colleague or a supplier. The email may contain a request for sensitive information or a link to a malicious website.
3. Whaling: This type of phishing attack targets high-level executives or high-value organisational targets. The attacker creates a personalized email that appears to be from a trusted source, such as a CEO or a board member, and asks for sensitive information or instructs the victim to perform an action, such as transferring funds to a fraudulent account.
4. Clone phishing: This type of attack involves creating a replica of a legitimate email or website and sending it to the victim. The email or website appears to be from a legitimate source but contains a malicious link or attachment. These can be particularly difficult to spot because they often will be very accurate and not contain many of the spelling or grammatical errors you may be used to seeing with some types of phishing.
5. Smishing: This type of attack involves sending a text message that appears to be from a legitimate source, such as a bank or a service provider. The message may contain a link to a malicious website or a request for sensitive information.
6. Vishing: This type of attack involves using voice communication, such as a phone call or a voice message, to trick the victim into providing sensitive information or performing an action.

In summary, phishing attacks can take many forms and can be challenging to detect. It's essential to be aware of the different types of phishing techniques and to take steps to protect yourself, such as avoiding clicking on links or downloading attachments from unknown sources, using two-factor authentication, and being vigilant about suspicious emails or messages.