How to Avoid Social Engineering Attacks

Social engineering attacks use deception to manipulate individuals into divulging confidential or personal information, including fake web sites and pretending to be a trustworthy person by email and on the phone.

In a social engineering attack, an attacker uses human interaction to manipulate a person into disclosing information. Social engineering attacks attempt to exploit our natural tendency to trust others in order to steal your information. The stolen information can be used to commit fraud or identity theft.

Web site Spoofing

Spoofing is the act of creating a fake web site to mislead individuals into sharing sensitive information. Spoofed web sites are typically created to look exactly like a legitimate web site published by a trusted organization.

Prevention Tips

- Pay attention to the web address (URL) of web sites. A web site might look legitimate, but the URL may have a variation in spelling or use a different domain.
- If you are suspicious of a web site, close it and contact the company directly.
- Do not click links on social media sites, pop-up windows, or non-trusted web sites. Links can take you to a different web site than their labels indicate. Typing an address in your browser is a safer alternative.
- Only give sensitive information to web sites using a secure connection. Verify the web address begins with “https://” (the “s” is for “secure”) rather than just “http://”.
- Avoid using web sites when your browser displays certificate errors or warnings.

Phishing

Phishing is when an attacker attempts to acquire information by masquerading as a trustworthy entity in an electronic communication. Phishing attacks are typically carried out through email, instant messaging, phone calls, and text messages.

Prevention Tips

- Delete email, text, and social media messages that ask you to confirm or provide sensitive information. Legitimate companies don’t ask for sensitive information this way.
- Beware of visiting web site addresses sent to you in an unsolicited message. Even if you feel the message is legitimate, type web addresses into your browser instead of clicking links.
- Try to independently verify with the company the details in a message.
- Utilize anti-phishing features available in your email client and/or web browser. Also, utilize an email SPAM filtering solution to help prevent phishing emails from being delivered.
- Do not open attachments from unknown senders or unexpected attachments from known senders.
- Be cautious of the amount of personal data you make publicly available through social media and other methods.

Report Suspicious Activity

Contact us immediately if you suspect you have fallen victim to a social engineering attack and have disclosed information concerning one or more of your accounts. Regularly monitoring your account activity is a good way to detect fraudulent activity.

Get the lastest information from our website. Scan the QR Code to go directly to this page.