Avoiding Social Engineering Attacks

Social Engineering

In a social engineering attack, an attacker uses human interaction to manipulate a person into disclosing information.

People have a natural tendency to trust. Social engineering attacks attempt to exploit this tendency in order to steal your information.

Once the information has been stolen, it can be used to commit fraud or identity theft.

Criminals use a variety of social engineering attacks to attempt to steal information, including:

- Website Spoofing
- Phishing Emails
- Phishing Phone Calls

This brochure explains the meaning of these common attacks and provides tips you can use to avoid becoming a victim.

Website Spoofing

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

Prevention Tips

Pay attention to the web address (URL) of websites. A website may look legitimate, but the URL may have a variation in spelling or use a different domain.

If you are suspicious of a website, close it and contact the company directly.

Do not click links on social media sites, pop-up windows, or non-trusted websites. Links can take you to a different website than their labels indicate. Typing an address in your browser is a safer alternative.

Only give sensitive information to websites using a secure connection. Verify the web address begins with "https://" (the "s" is for "secure") rather than just "http://".

Avoid using websites 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 (SMS).

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 website 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 any details given in a message directly with the company.

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. If you notice unauthorized transactions in your account, notify us immediately.

How To Report

If you need to report suspicious activity, please contact:

Central Willamette Credit Union
(Name of Financial Institution)

(541) 928-4536
(Financial Institution Phone Number)

https://www.centralwcu.org/contact
(Financial Institution Web Address)

Learn More

To learn more about information security, visit any of the following websites:

- OnGuardOnline.gov
- StaySafeOnline.org
- BBB.org/Data-Security
- US-CERT.gov