Protect Yourself from Phishing Attacks

SUMMARY: Phishing attacks are a popular way for cybercriminals to bypass your security measures and trick you into providing personal and financial information.

Technology is getting safer and smarter, which means cyber criminals are focusing their attention on taking advantage of the most obvious weakness**: human error.**

With sophisticated techniques, these scam artists mount **phishing** attacks – messages, usually emails, designed to manipulate and trick people into providing personal and financial information.

How phishing works

Most phishing attacks are in the form of an email, designed to look like they are from a person or a company you trust, such as the Social Security Administration. Usually, the email informs you there is a problem, and you need to take immediate action. Other times, the email invites you to claim a reward. The messages are crafted to play on your emotions, by fear or excitement, so that you act before thinking.

Clicking a link in the email results in a download of malware or directs you to a website where you are prompted to provide information, such as an account number, Social Security Number, or other personal information. Criminals can lock your computer through malware until you pay a ransom. The criminals can get credit in your name or access your accounts with your personal information.

What to look for

- Check the sender's actual email address, rather than just the display name. If the names don't match or the sender's address is from an unknown URL, it's suspicious.
- Hover your mouse over a link to see the real address. If the URL is different than the link description, it's a sign of phishing. If the address has "http:" instead of "https:" at the beginning, it's not a secure site.
- Poor writing and typos are the hallmark sign of phishing attempts.
- An urgent tone used to get you to act quickly without thinking through the details of the message is a typical strategy. Look for phrases like "urgent," "immediate," or "action required."

What to do If you receive a phishing attempt:

- Avoid clicking on any links.
- Notify the business the phishing scammer impersonated so they can investigate. Be sure to use a phone number you can independently verify is real. You may be asked to forward the email to them as well.
- Forward the email to the Federal Trade Commission at spam@uce.gov.
- Delete the email and block the sender.

- Review account statements and your credit reports regularly and take action if you notice any irregularities by contacting the creditor.

If you become a phishing victim:

- Alert your financial institutions immediately.
- Close fraudulent accounts.
- Place fraud alerts on your credit files with the three credit reporting agencies: Equifax, Experian, and Transunion.
- File a report with your local police department and the Secret Service, which investigates financial cybercrimes.

Source: TDECU Security and Fraud Protection