Social Engineering and How to Protect Yourself

Social Engineering is a non-technical method of intrusion hackers utilize. It relies heavily on human interactions and behaviors. The most prevalent type of Social Engineering attack that occurs to customers is a phishing attack. Phishing is the attempt to acquire sensitive information such as usernames, passwords, credit card details, financial information, and sometimes money for malicious reasons by masquerading as a trustworthy source.

Phishing attacks can occur by email, text, instant messaging, social media, and/or by phone.

Here are a few ways you can prevent yourself from falling victim to social engineering techniques:

- Don't respond to ANY email or social networking post or message that advertises free items, asks for money or to utilize your account for a monetary transaction, requests you to reveal user names and passwords, asks for your phone number and/or address, or other confidential information.
- Don't assume that an unsolicited phone call or message is actually from a trusted source. Thieves can research your purchases or donations, then poses as a business or charity.
- Verify. If someone on the phone or a message is telling you there is a problem with your online banking account don't give them additional information to "fix" the problem. Hang up or delete the email and check those accounts directly by logging in normally or calling a published customer service number.
- Be conscious of what can be learned about you. Thieves are very good at digging out the basic security questions such as mother's maiden name or the model of your first car.
- Even the most innocent attachments can be infected with malware. If you aren't certain the message came from a legitimate source DO NOT OPEN it without verifying. Call the source and ask if they sent an email with an attachment.