INFOSEC

ADVISORY BULLETIN

First Quarter 2017

Social Engineering and Phishing:
What are they and how can they affect my business and me?

The Basics:

Social engineering: An attempt to manipulate people into divulging confidential information

Phishing: One of the most common forms of social engineering and a technique used to fraudulently obtain private information, typically in the form of emails directing the user to click on the link in the message. The link is often intended to steal user credentials (user ids & passwords) and is also used to deliver malicious software, such as viruses, to your computer.

Phishing emails appear to be coming from a legitimate business or recognized user (the real name of the sender/business is typically spoofed. Spoofing, in general, is a fraudulent or malicious practice in which communication is sent from an unknown source disguised as a source known to the receiver. Spear phishing is a more targeted email attack sent to a select number of users and a Whaling attack, also known as Business Email Compromise (BEC), is an even more targeted variation of spear phishing that targets high-profile executives or used in wire fraud attempts.

Real Life Impact:

- You receive a phishing email from PayPal. You click on the link and without realizing it, you give out your credentials to the hacker. Here is what the hacker can do with it:
    - Log in to your PayPal account and if you linked your checking account, the adversary can siphon all your savings to his bank
    - Use the same credentials at major bank websites and credit card companies. If they succeed, they can transfer your funds to their account

Copyright 2017American Land Title Association. All Rights Reserved.

- Use the same credentials at online mail sites (Google, Yahoo, Outlook, etc.). If they succeed, they can monitor your email activity and use your e-mail account without your knowledge and potentially use it to change wiring instructions and divert funds.
- Use the same credentials at websites for major insurance carriers. If successful, they can potentially get your social security number
- Use same credentials to potentially gain access to all your social media accounts. If they succeed, they can monitor your email activity and use your email account without your knowledge and potentially use it to change wiring instructions and divert funds

How to Protect Yourself:

- If you receive an email that has a link in it, even if you're expecting it and you trust the sender, never click on the link. Go to the website directly to log in. Then, delete the message
- Vendors no longer send invoices through email as attachments and most reputable shopping sites expect you to view the invoice and status of shipping on their website, and will never send you attachments.
- Use unique passwords for every website you visit. Use password managers to help you generate strong passwords and them. Password managers are inexpensive and are easy to use.
- Change your passwords frequently. Many password managers will assist you with that. Even if your password is unique and hard to guess, you should still change it frequently. Many security breaches go unnoticed or unreported for a long time, and hackers may be using your old password without your knowledge.
- Use reputable cloud mail services (i.e. Office365, Outlook.com, Google). They all have many security features enabled by default and more available as add-ons.
- Check your email for signs of compromise. If you are suspect something is amiss, check your sent and deleted items for messages you didn't send.
- Watch for look-alikes in the sender's address. Hackers and cyber criminals frequently use similar domains by replacing vowels with numbers or inserting one letter within a long domain name.
- Keep your antivirus (AV) current and don't forget your mobile devices. There are plenty of AV products for mobile devices.
- Keep your systems patched.
- Use multifactor authentication (e.g. tokens) in addition to your passwords, whenever possible. Even if your passwords are stolen, the second factor is much harder to circumvent. Two-factor authentication is available for many e-commerce retailers, most banks, social media, and e-mail platforms.

It's important to note that social media is widely used by cyber criminals for social engineering attacks and credential theft. Protect yourself:

- Educate yourself about the danger of social engineering attacks associated with social media
- Keep your personal and business social lives separate.
- Don't accept social media invitations from people you don't know. Just because someone is a member of the same group on the LinkedIn, does not mean you have something in common.

- Avoid suspicious content. URL shorteners used on most social media platforms are convenient but dangerous. You never know where it will redirect you. Treat all URL shorteners as potential threats.
- Don’t download third-party applications to just view or access the content. If someone sends you a picture and you need to install an application to view it, it is most likely malicious
- Don’t trust, and always verify. Some larger social media providers have added “verified account” indicating their legitimacy. Otherwise, don’t trust everything you see on the social media.
- Don’t underestimate the age of your mobile device. Apple makes security updates available for most of their platforms, where Google relies on OEM partners to deliver updates. Consequently, a 2015 study by the University of Cambridge found 87.7% android devices are exposed to at least one of 11 known critical vulnerabilities.