Don't Get Taken on a Phishing Expedition

Phishing is a fraudster’s attempt at gaining access to your usernames, passwords, and financial information by posing as a trustworthy or legitimate business. A common phishing scam looks like an email from a social media website, online auction website, payment processor, or financial institution. The message will attempt to gain your trust by claiming that you already have a business relationship with the sender, and that the company would like to verify some of your information in order to continue that relationship.

For instance, you may receive an email claiming to be from PayPal. The email message might contain the PayPal logo. The sender’s email address may even include the words “Pay” and “Pal.” The message will explain that “PayPal” is updating their system, or that they have received inquiries about their customer support system, and they are working to improve their service. It will all sound very convincing. At the end of the email, there will be a place for you to click on a link in order to verify your information. However, the link might take you to an unofficial website, and may ask that you download certain software updates to be sure that your information is stored correctly. Once you submit your information or download the program, the fraudster has all the information he or she needs to commit identity theft.

Phishing attacks are becoming more widespread and vicious as more service providers move online. While it may be convenient for you to be able to pay your electric bill online, or to transfer money from your bank account to your PayPal account with the click of a button, fraudsters now have many masks that they can hide behind. Clever scammers have found ways to mimic the authentic looking emails that you receive from all types of companies, from your utility company to your bank.

Recently, over 2 million people across the country received an email notifying them that their online order through the “Wallmart” website was being processed (they must not have noticed the misspelled company name). Thousands of individuals clicked on the link, allowing hackers to infect the computer with malware, or allowing a scammer to steal the individual’s usernames and passwords.

So what can you do to protect yourself from these types of phishing attacks? The Federal Trade Commission recommends that you follow these action steps (via www.onguardonline.gov):

- Use trusted security software and set it to update automatically.
- Don’t email personal or financial information. Email is not a secure method of transmitting personal information.
• Only provide personal or financial information through an organization's website if you typed in the web address yourself and you see signals that the site is secure. A secure site will have a URL that begins https (the "s" stands for secure). Unfortunately, no indicator is foolproof; some phishers have forged security icons.

• Review credit card and bank account statements as soon as you receive them to check for unauthorized charges. If your statement is late by more than a couple of days, call to confirm your billing address and account balances.

• Be cautious about opening attachments and downloading files from emails, regardless of who sent them. These files can contain viruses or other malware that can weaken your computer's security.

• Protect your passwords, and treat your personal information like cash.

For more information on consumer fraud and scams, including helpful preventative tips and contact information for other community resources, contact Stetson University College of Law's Elder Consumer Protection Program by e-mail at elderconsumers@law.stetson.edu, or by telephone at (727) 562-7888.