

FEAP NEWSLETTER

A Series of Educational Articles from your Faculty and Employee Assistance Program

October is National Cyber Security Awareness Month

By Owen McKenzie, ACSW, CEAP
Director, FEAP



The Web is an incredible community with much to offer, but its many benefits come with risks. This is just one of the many forms of identity theft. For example, have you seen one of the following email headers?

“We suspect an unauthorized transaction on your account. To ensure that your account is not compromised, please click the link below and confirm your identity.”

“During our regular verification of accounts, we couldn’t verify your information. Please click here to update and verify your information.”

This is a scam called “phishing” — and it involves Internet fraudsters who send spam or pop-up messages to lure personal information (credit card numbers, bank account information, social security number, passwords, or other sensitive information) from unsuspecting victims.

According to the Federal Trade Commission (FTC), the nation’s consumer protection agency, phishers send an email or pop-up message that claims to be from a business or organization that you may deal with — for example, an Internet service provider (ISP), bank, online payment service, or even a government agency. The message may ask you to “update,” “validate,” or “confirm” your account information. Some phishing emails threaten a dire consequence if you don’t respond. The messages direct you to a website that looks just like a legitimate organizational site. But it is not. It is a bogus site whose sole purpose is to trick you into divulging your personal information so that the operators can steal your identity, run up bills, or commit crimes in your name.

The FTC suggests these tips to help you avoid getting hooked by a phishing scam:

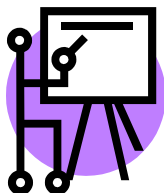
- **If you receive an email or pop-up message that asks for personal or financial information, do not reply.** Also, do not click on the link in the message. Legitimate companies do not ask for this information via email. If you are concerned about your account, contact the organization mentioned in the email using a telephone number you know to be genuine.
- **Area codes can mislead.** Some scammers send an email that appears to be from a legitimate business and ask you to call a phone number to update your account or access a “refund.” If you need to reach an organization that you do business with, call the number on your financial statements or on the back of your credit card. In any case, delete random emails that ask you to confirm or divulge your financial information.

- **Use anti-virus and anti-spyware software, as well as a firewall, and update them regularly.** Some phishing emails contain software that can harm your computer or track your activities on the internet without your knowledge.

Anti-virus software and a firewall can protect you from inadvertently accepting such unwanted files. Anti-virus software scans incoming communications for troublesome files. Look for antivirus software that recognizes current viruses as well as older ones, can effectively reverse the damage, and that updates automatically.

- **Do not email personal or financial information.** Email is not a secure method of transmitting personal information. If you initiate a transaction and want to provide your personal or financial information through an organization's website, look for indicators that the site is secure, such as a lock icon on the browser's status bar or a URL for a website 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 your credit card company or bank to confirm your billing address and account balances.
- **Be cautious about opening any attachment or downloading any files from emails you receive,** regardless of who sent them. These files can contain viruses or other software that can weaken your computer's security.
- **Forward spam that is phishing for information** to spam@uce.gov as well as to the company, bank, or organization impersonated in the phishing email. Most organizations have information on their websites about where to report problems.
- **If you believe you have been scammed, file your complaint at [ftc.gov](https://www.ftc.gov),** and then visit the FTC's Identity Theft website at www.consumer.gov/idtheft. Victims of phishing can become victims of identity theft. While you cannot entirely control whether you will become a victim of identity theft, you can take some steps to minimize your risk. If an identity thief is opening credit accounts in your name, these new accounts are likely to show up on your credit report. You may catch an incident early if you order a free copy of your credit report periodically from any of the three major credit bureaus. See www.annualcreditreport.com for details on ordering a free annual credit report.

For more information regarding email scams, go to ftc.gov/spam.



The University of Virginia Community Credit Union is a local resource which will be conducting free seminars during the month of October on **Identity Theft: Prevention & Response**. You can reach them via the following link: https://www.uvacreditunion.org/cybersecurity_aware2007.html

All forms of identity theft continue to be on the rise, so please exercise caution. If you have any questions regarding this important topic or other personal or workplace issues, please do not hesitate to call us at (434) 243-2643. You can also visit us on the web at www.uvafeap.com.