

Protect Yourself: Phishing and other online scams"

This is the fourth and final message in a series of bulletins for National Cybersecurity Awareness Month. Each bulletin will address a topic in computer security that will help you keep your computer and your personal information safe. This week's topic covers how to spot and avoid phishing attacks and other types of online scams.

Phishing is when a criminal attempts to trick you into providing your social security number, bank account information, credit card numbers, and similar types of information. The criminal then uses this information to steal money from you. The most common form of phishing involves a message that appears to come from a bank. The message will inform you that you need to click on a link and input information about your account, such as your account number and password. If you click on the link, it will look a lot like your bank's actual website. However, since the phisher controls the link, your information will be going wherever the phisher wants it to go. Once they have your account information, the phisher can login to your bank account and take your money, or use the information to attempt to steal your identity.

If you receive a phishing letter, the simplest thing to do is to simply delete it. Alternatively, you can forward the email to reportphishing@antiphishing.org. This is a non-profit organization that collects information about phishing reports. Be sure that you do not click on any links or pictures in the suspected email. Rather, if you suspect that the email might be legitimate, open your web browser and type in the address yourself. For example, if you receive a email from Citibank asking for you to go to <http://citibank.com>, instead of clicking on the link (which could point to a different address that looks like Citibank's site), open your web browser and type in <http://citibank.com>. Also remember that your bank will send communications via postal mail, rather than email, if the information is important.

Another common online scam is known as a Nigeria 419 scam or an advance fee fraud scam. In the most common forms of this scam, you will receive a fax or email from a stranger claiming to have access to a large sum of money, but requiring your help to get the money out of the country. In exchange for your help, the stranger will give you a percentage of the money, which is usually millions of dollars. If you agree to help, the stranger will ask you to send over various small sums of money to help get the money out of the country. This is the advance fee portion of the scam, and any money that is sent over will never come back. The stranger keeps asking for additional sums of money, always promising that this is the last payment before the big payoff. The scam is also known as a Nigeria 419 scam as the scam most commonly is operated out of Nigeria, and 419 is the section of the Nigerian penal code that should cover this crime but is rarely enforced.

If you receive what appears to be a Nigeria 419 scam (which does not always involve Nigeria in the letter, but will involve a foreign country), the simplest thing to do is to simply delete it. If you would like to report it and have not suffered a financial loss to the scam, forward a copy to 419.fcd@uss.s.treas.gov. If you fallen suffered a financial loss to this scam, contact your local United States Secret Service office.

If you have additional questions, you may want to check out Loyola's Information Security website at http://www.luc.edu/is/security/protect_yourself.shtml or send your questions to InfoSecurity@luc.edu.

Hopefully these bulletins have helped to raise your security awareness and will help you to stay safe while you're online.