Jennifer M. Joyce
& The Circuit Attorney's Office

Fraud Bulletin

Gone "Phishing?" Watch Out, There's Danger Under the Surface!

Recently, the personal email account of a Circuit Attorney's Office employee was hit with numerous phishing messages. "Phishing" is the term used when internet fraudsters send emails impersonating a legitimate business to trick you into giving out your personal or financial information. Here are recent examples of the emails received by our colleague:

- An email from Order-update@amazon.com which said "Your order has been sucessfully cancelled."
- A message from YouTubeservice@youtube.com reported "The video you ordered is ready to be viewed."
- A "notification" from accountnotify@verizon.com that said "Your bill is ready and amounts to $1,900."
- An administrator at noreply@message.myspace.com wanted "to verify your email address."

Our employee did not make and then cancel an Amazon order, did not order a video from YouTube, does not owe Verizon any money and is not a MySpace user. All of these messages had embedded links that the recipient was told to click on for more information. An internet search showed they are all likely phishing attempts, designed to entice you to click on a link that sends you to a "spoofed" website. These sites pose as the internet addresses of legitimate companies. There, you are asked to provide personal information. If you give this information without realizing it is a scam, you'll likely be a victim of identity theft and account takeover fraud. To make matters worse, your computer is also at risk of being infected with malware.

According to the June 2012 Consumer Reports magazine, over 9 million U.S. households were duped by phishing schemes in the last 12 months and nearly 30 million homes had malware installed on their computers. Don't be one of them!

OnGuardOnline.gov offers these tips to avoid phishing scams:

- Be cautious of any unsolicited emails seeking personal information.
- Use trusted security software and set it to update automatically. The suspicious emails sent to the CAO employee were automatically placed in his "spam folder."
- Do not click any links or open any attachments in unsolicited emails.
- Forward the emails to spam@uce.gov and to the actual company or reported agency impersonated in the email. You can also report phishing emails to the Anti-Phishing Working Group at reportphishing@antiphishing.org. Once you've done this, make sure to delete the message.