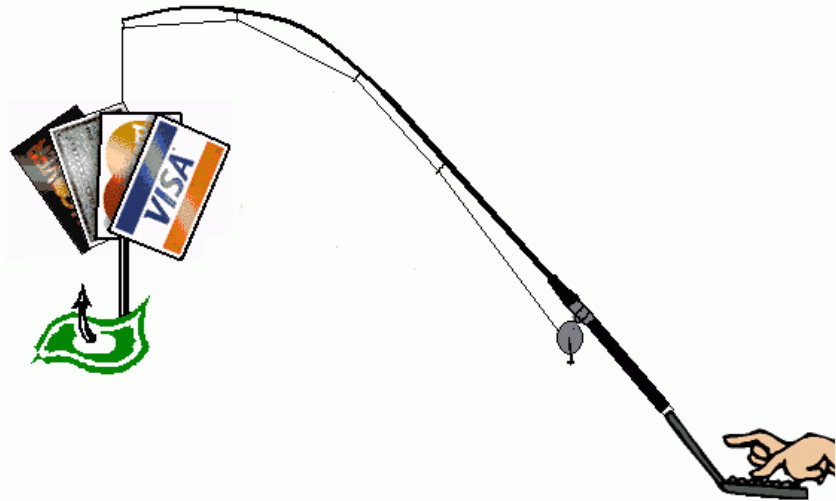


Scammers are 'Phishing' for Your Money-Don't Take Their Bait!

Phishing is a high-tech scam that uses spam to deceive people into disclosing their credit card numbers, bank account information, Social Security numbers, passwords, and other sensitive personal information.



Email and Internet users are reporting a significant escalation in the number and sophistication of these scams.

These deceptive messages, most often sent via email (but also via instant messenger, and cell phones), fake (spoof) the appearance of popular auction, financial, merchant, and other company Web sites in an attempt to commit identity theft. **These spoofed messages/sites are very convincing and often look exactly like the legitimate sites.** Currently, the most prolific appear to be sent from companies such as US Bank, eBay, Citi, Amazon, and PayPal. There are many other accounts/companies targeted as well.

If you receive an email message requesting you verify personal, financial, password, or other information, **DO NOT** reply, **DO NOT** click on a link, and **DO NOT** follow the instructions in the message, regardless of how authentic the message appears. What you *should* do is forward the message to the Federal Trade Commission (spam@uce.gov), and to the targeted company's fraud unit (see below), then delete the message.

Email is NOT a secure protocol, so you should **NEVER** send private or sensitive information using email. You should also NOT respond to any request for personal or sensitive information (reputable companies will not even ask.) If you are in doubt as to the legitimacy of a message, **never click on an email link**; instead, go directly to the home page of the company supposedly requesting the information and validate the request.

For example, if you have an account with eBay and receive a message instructing you to update your account information via a web link or email form, **it is a scam**. If eBay really needed you to update your information, they would send you a message instructing you to go directly to the legitimate home page by typing www.ebay.com in the address bar of your browser, and then login to your account from the home page. They would NOT include a link or form in the message itself.

Addresses to report fraud targeting some of the major companies are:

eBay: spoof@ebay.com

US Bank: fraud_help@usbank.com

Citi: emailspoof@citigroup.com

PayPal: spoof@paypal.com

Amazon: stop-spoofing@amazon.com

This is currently one of the fastest growing Internet threats, and there is little that can be done *technically* to prevent this. On the Sinclair Campus, setting up SpamAssassin to filter your Outlook mail messages can help you identify these spoofed messages...if SpamAssassin identifies the message as spam, it is likely not legitimate. Instructions are here:

http://intranet.sinclair.edu/its/itswebsite/it_policies/procedures/otlk/spam_assassin/spamassassininstructions.htm

Want to learn more? Here are some excellent resources on spoofing and phishing:

<http://pages.ebay.com/education/spoof/tutorial/>

<http://www.citi.com/domain/spoof/learn.htm>

http://www.usbank.com/cgi_w/cfm/promo/personal/fraud_email_info_and_help.cfm

Daniel V. O'Callaghan, Jr., CISSP
CISO, Sinclair Community College
937-512-2452
daniel.ocallaghan@sinclair.edu