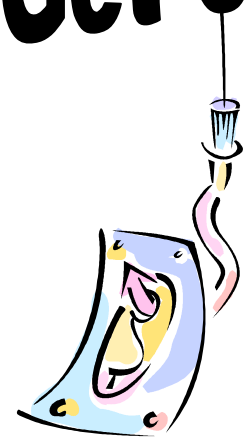
Phishing - Don't Get Caught!



What is "Phishing"? Phishing is an e-mail or other communication impersonating a legitimate organization and trying to get you to volunteer personal information such as bank account numbers or e-mail passwords. Phishers often impersonate banks, PayPal, eBay, credit card companies, and computer Help Desks. Often phishers say there is something wrong with your account, and supplying the information will help them fix it — but it's a **SCAM**! In addition to e-mailed phishing attempts, you may encounter phishing on Facebook, MySpace, Twitter, instant messages, legitimate websites, and even phone calls.

What happens with phished information? Your personal information in the wrong hands can do a great deal of damage, both to you as an individual and to our campus computer systems. It can be used for a variety of fraudulent purposes, such as

- Withdrawing funds from your bank account
- Charging purchases to your credit card
- Opening new credit accounts in your name and charging to the limit
- Using your e-mail account to launch more spam/phishing attacks. The e-mail servers can get so flooded with the resulting spam that service can be very significantly impaired. Successful phishing incidents have actually resulted in e-mail delays on our own campus, impacting everyone's ability to receive timely e-mails and do their jobs effectively. Many colleges, universities, businesses, and other organizations around the country are struggling to control this growing problem.

(continued, next page)

How do I protect myself?

To protect yourself and our campus community:

- Be suspicious of any communication that asks for personal information such as account numbers or passwords, especially those that threaten your account is closed, that you have won a prize, etc.

- Never respond to e-mailed phishing attempts — just delete as spam.

- Never click on website links provided, asking you to go to a particular website.

- Always double-check the true identity of anyone asking for sensitive information. Use Google or your account statements to find legitimate web addresses of the organization that appears to be sending the communication.

- Keep in mind that communications from UIndy Information Systems will always be signed by an employee, and staff will **never** ask you for your password.

- Keep your anti-virus software up-to-date.

- **Additional information on recognizing and dealing with phishing** is available at http://is.uindy.edu/faq - Viruses, Spyware, & Computer Health section.

Phishing Facts *

- **886** – The average dollar loss per Phishing Victim (Gartner, Dec 17, 2007)
- **3.6 Billion** – The total dollar loss of all phishing victims over a 1 year period (Gartner, Dec 17, 2007)
- **3.2 Million** – The number of people who fell victims to phishing scams over that same 1 year period (Gartner, Dec 17, 2007)
- **8.5 Billion** – The estimated number of phishing e-mails sent world-wide each month (SonicWALL, 2008)
- **32,414** – The number of phishing web sites that were operational in May 2008 (Anti-Phishing Working Group)

* from http://www.sonicwall.com/phishing/ accessed on 12/12/08