



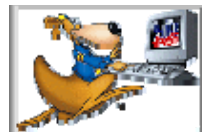
Phishing Prevention

- Be suspicious by default
- Scrutinize URL's: verify target links
- Do not visit sites via links – use bookmarks or type in the URL
- Disclose your email address only when necessary
- Check to make sure the web site is using encryption (https)
- Do not be put at ease by language that suggests a concern for your security
- Maintain a pop-up blocker
- Know common formats of fraudulent links
- Never respond to requests for personal information via email or in a pop-up window
- Forward phishing messages to spam@uce.gov



What to do if you get hooked

- Alert the credit bureaus - they will put an "alert" on your file for 90 days
- Request a copy of your credit report from www.annualcreditreport.com. - you are entitled to one free report per year
- Require written notice to extend credit
- Inform the impersonated company or person
- Close the account and reopen a new one
- Report fraud to www.fraud.org
- Notify the credit bureaus
- File a police report
- File a complaint with the FTC at ftc.gov or call the FTC at 1-800-FTC-HELP



Software Training
April 2006

WANTED Phil the Phisher



Captain of the S.S. Not-Quite-ebay, he trolls the seas of the Internet, casting his nets of email scams on unsuspecting users. If his clever words fool them into believing he represents their bank or a real person in need, he reels them in and steals their information and their identity.

Don't let Phil get his hooks in you – delete his suspicious emails right away!

*The University of Akron
April 2006*

Definition of Phishing

Phishing is the process by which someone obtains private information through deceptive or illicit means in order to falsely assume another person's identity.

The Phisher will use spoofed emails to lead the recipient to counterfeit websites. Once here, the victim is tricked into divulging credit card information, account usernames and passwords, social security numbers, etc.

Recognizing Phishing

Three main components:

1. Attempt to build **credibility**
 - a. Spoof a real company
 - b. May or may not have an account with them
2. Create a **reason to act**
 - a. Sense of urgency, plausible premise – requires quick response
3. Require a **call to action**
 - a. A link or button will appear in the email message, making it easy to respond

The following items may also be present:

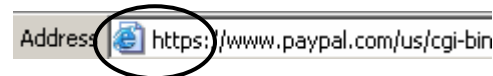
- Official-looking Logo
- Will employ a method to establish trust
- Genuine-looking fine print at the bottom



Identifying a Valid Site

Note the following items which identify the site as being secure:

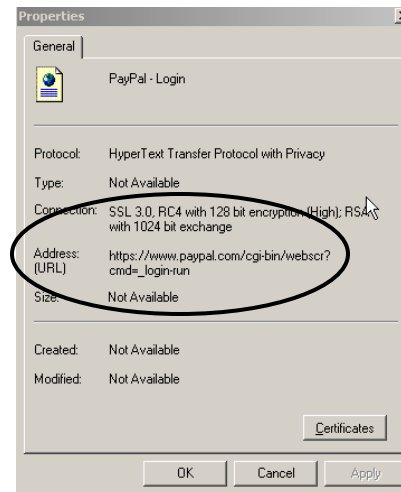
1. The address line displays **https**



2. The **lock** icon located in the lower right status bar:



To identify the web address select **File-Properties** from the menu to reveal the actual web address:



Resources

Office of General Counsel – Identity Theft Web Page	http://www.uakron.edu/ogc/PreventiveLaw/identitytheft.php
Anti-Phishing Working Group	http://www.antiphishing.org/index.html
Identity Theft Website	http://www.consumer.gov/idtheft
Consumer Fraud Reporting	www.consumerfraudreporting.org
Internet and Telemarketing Fraud	http://www.fraud.org
The full Phishing IQ Test	http://survey.mailfrontier.com/survey/quiztest.html
Identity theft affidavit	http://www.ftc.gov/bcp/online/pubs/credit/affidavit.pdf
Complaint to FTC	https://rn.ftc.gov/pls/doi/widtpubl\$.startup?Z_ORG_CODE=PU03
Credit Report	http://www.annualcreditreport.com