

ANTI-PHISHING TOOLS

There are a number of utilities available to help warn you of suspicious web sites. Use one or more for your protection.

- The Netcraft Toolbar displays information about a web site including whether it is new (typical of phishing) and which country hosts it. The Netcraft Toolbar also works like a neighborhood watch community, blocking access to reported phishing sites.

<http://www.netcraft.com>



- The Google Safe Browsing Extension will warn you when a “phishy” site has been detected, and block you from entering information into the site.

<http://www.google.com/tools/firefox/safebrowsing/>



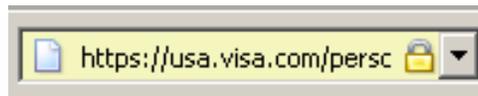
- Earthlink ScamBlocker provides an easy-to-see security rating for each web site you visit, based on a blacklist of fraudulent sites.

<http://www.earthlink.net/software/free/toolbar/>



ANTI-PHISHING TECHNIQUES

- Never click on links directly from an e-mail! Type the address into the address bar or go to the institution’s web site and navigate to the correct location.
- Check the properties of web pages before entering information. You can check the properties from the file menu or by right-clicking on the web page and selecting properties.
- Secure web sites use a technique called SSL (Secure Socket Layer) that ensures the connection between you and the web site is private. This is indicated by “https://” instead of “http://” at the beginning of the address AND by a padlock icon which must be found either at the right end of the address bar or in the bottom right-hand corner of your browser window. A padlock appearing anywhere else on the page does not represent a secure site.



WHERE DO I GO FOR MORE INFORMATION?

Visit our web site at security.rit.edu to read the security standards, get the schedule for our Digital Self Defense workshops, or find out more ways to protect yourself.

This work is licensed under the Creative Commons Attribution-NonCommercial-ShareAlike 2.5 License.

RIT INFORMATION SECURITY
Phone: 585-475-4122
E-mail: infosec@rit.edu
Web: <http://security.rit.edu>

AVOIDING IDENTITY THEFT ONLINE



Detecting Online Scams and Phishing



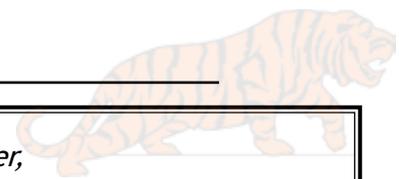
**INFORMATION
SECURITY**

Issued by the RIT Information Security Office

Revised 8/30/2006

Avoiding Identity Theft Online: Detecting Online Scams and Phishing

INTRODUCTION



*Dear Paypal User,
We've recently noticed one or more at-
tempts to log into your account from a
foreign IP address. If you did not initiate
the logins, please visit Paypal at:
<http://paypal-secure.com>
Thank you,
Paypal Security*

Have you received an email like this? Did you click on the link and enter login information?

You've been phished!

According to a 2003 Computer Use and Ethics survey, some RIT students have been victims of identity theft.

Phishing is a commonly-used technique in identity theft. We've all received phishing emails or instant messages that appear to link to a legitimate site. These e-mails and web sites are designed to capture personal information, such as bank account passwords, social security numbers and credit card numbers.

This pamphlet provides tips on identifying phishing attempts and suggests a number of tools and techniques you can use to defend yourself and others from them.

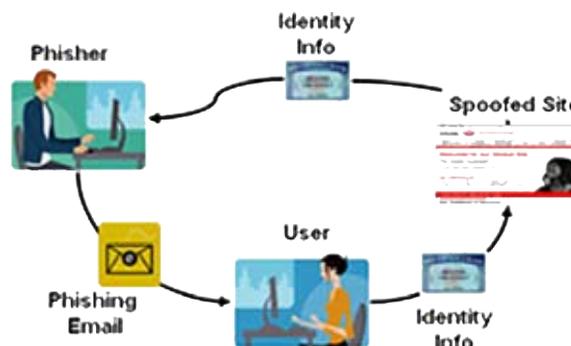
HOW BIG IS THE THREAT?



Email phishing really picked up in August of 2003. It has grown astronomically, with phishing e-mails peaking in May 2005 at more than 9,000,000 attempts. Losses to phishing attempts may be as high as \$500M every year.

HOW PHISHING WORKS

- Phishers send out millions of e-mails disguised as official correspondence from a financial institution, e-tailer, ISP, etc.
- You receive the phish in your email.
- After opening the email, you click on the link to access your financial account.
- Clicking on the link takes you to a web site that looks just like a legitimate site.
- At this point, you enter your account and password information, which is captured by the person who sent out the phish.



Phishers typically attempt to impart a sense of urgency, urging you to act quickly to address the problem referenced in the phishing email.

DETECTING A PHISH



Phishing emails used to be easy to recognize because of their poor spelling and grammar. Now, phishing emails are often indistinguishable from official correspondence.

Phishing sites may also be difficult to distinguish from legitimate sites, because of their use of these techniques:

- **URL masking**—phishing emails may display a link that appears to go to one site, but in reality goes to another.
- **Copying of official e-mail**—phishers may simply copy an official e-mail from a bank or retailer, and edit that e-mail for their own purposes before sending it to you.
- **Cybersquatting**—phishing sites may rely on similar URLs, such as `googkle.com`, `ebay-secure.com`, `upgrade-hsbc.com` to fool users.
- **Use of @ symbol**—the phishing URL may include the @ symbol somewhere within the address. (When reading an Internet address, browsers ignore everything to the left of the @ symbol, so the address `ebay.com@fake-auction.com` would actually be “fake-auction.com.”)

Phishing techniques are becoming more difficult to detect as phishing attempts become more complex. Some links may actually send you to a legitimate site, and use some other technical means to capture your information!