safe practices

- It’s not always safe to just click on a link! Enter or copy the link into the address bar or go to the institution’s website and navigate to the correct location as you normally would.

- Check the properties of websites 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 website is private. The use of SSL 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.)

anti-phishing tools

There are a number of tools available to help warn you of suspicious websites. Use one or more for your protection. For an updated list of anti-phishing tools, visit the RIT Information Security Phishing page at http://rit.edu/security/content/phishing.

take a phishing quiz

Do you think you can identify a phishing attempt successfully? Find out by taking the SonicWall phishing quiz at http://www.sonicwall.com/furl/phishing/.

get informed

Visit the RIT Information Security website to read the security standards, get the schedule for our Digital Self Defense workshops, access security tools and software, or find out more ways to protect yourself.

RIT INFORMATION SECURITY
http://rit.edu/security
infosec@rit.edu
(585) 475-4123

DIGITAL SELF DEFENSE:
avoiding identity theft online

Detecting Online Scams & Phishing

Revised 7/17/2013
Introduction

Dear Webmail User,
You’ve recently exceeded your e-mail quota. Please provide your login name and password within 24 hours or you will no longer be able to login to your account.

Thank you,
The Webmail Team

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

If you did, you’ve been phished!

Phishing is a common technique for identity theft. We’ve all received phishing emails or instant messages that appear to link to a legitimate site. These emails and websites are designed to capture private information, such as bank account passwords, social security numbers and credit card numbers.

RIT receives many phishing attacks each year. Some phishing attempts have targeted RIT Computer Account passwords. After the accounts were compromised, the attacker uses them to send out thousands of pieces of spam.

Phishing is also used to trick employees into providing login information. Attackers often use this technique to gain access to corporate “secrets” and other confidential information.

How phishing works

- Phishers send out millions of emails disguised as official correspondence from a financial institution, e-tailer, ISP, etc.
- You get the phishing contact in your email.
- After opening the email, you click on the link to access your account.
- The link takes you to a fake (“spoofed”) website that looks like the legitimate site.
- At this point, you enter your account and password information, which is captured by the person who sent out the phish.
- Some phishers will actually log you into the real site after capturing your information, so you never realize you gave your login information to a spoofed site.
- Phishing sites are also used to deliver malware. You may discover you’ve both compromised your private information and installed malware on your computer by responding to the phishing attempt.

Detecting a phish

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

Most phishing attempts try to create a sense of urgency to provoke a quick response. For example, many phishing emails threaten negative consequences unless there’s a quick reply.

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

URL masking/cloaking: phishing emails may display a link that appears to go to one site, but in reality goes to another.

Modifying a legitimate email: phishers may simply copy an official email from a bank or retailer, and edit that email 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 the @ 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.”

http://rit.edu/security