Identifying Phishing Scams

IT Services Tech Talk

May 4, 2010

What is Phishing?

- Fraudulent attempt to obtain personal or sensitive information, such as usernames, passwords, and credit card numbers
- Sender claims to be a trustworthy entity, often spoofing characteristics of the message to appear legitimate
- Typically carried out via email or instant messaging

What's the Problem?

- Compromised accounts used to send thousands of spam messages
- Scammers may read or delete your email
- Scammers may go on to other sites

Characteristics of a Phishing Email

- Urgent call to action – do this now, or something bad will happen
- Sender appears to be a legitimate entity – IT department, bank, credit card company, web site, etc.
- In some cases, language may be non-standard

Spoofing Emails

- Spoofing the sender address is trivial – it's as easy as writing a fake return address on a letter
- Signs of forgery are present, but hidden in the email header information
- If you reply to a message, it goes to the "reply-to" address, *not* the "from" address

Spoofing Web Links

- Links may go to a different destination than they appear.
- Scammers may register sites with similar names to aid their scam, e.g. www.ammazon.com
- Some links may contain hostnames within the folder path, e.g. www.mbfx.cn/wabash.edu/login.htm

Spoofing Web Sites

- It is easy to spoof web sites. Any web page can link to images on other sites, or even copy entire pages

How to Identify a Scam

- If a message asks you to send your password or other information via email, you can be absolutely certain it is a scam.
- Watch for odd language, strange email addresses and links, and anything suspicious
- Check links carefully before clicking; if you are in doubt, type them in your browser rather than clicking a link
- Become familiar with secure SSL connections

Verifying Messages

- If you are ever unsure of a message, contact the Help Desk for assistance
- Don't reply to a message asking if it's a scam
- Be cautious of phone numbers in email messages – they may be spoofed too
- Companies and organizations may have information on their web sites describing scams currently in circulation

Don't Bait the Phishers

- If you get a scam, simply delete it. Don't file it or leave it in your mailbox – you may come across it later and think it is legitimate
- Don't reply to scam messages, even to say you weren't fooled. This lets the scammers know they have a valid email that someone actively checks, and will encourage more contact