Don’t Fall for the Bait

Recognizing Phishing Scams, Fraudulent E-mails and Protecting Yourself

What are Phishing Scams?

Phishing is e-mail or instant messages that look like they're from a reputable company to get you to click a link. Their goal is to retrieve user's personal and account information. These messages can look like the real thing, right down to a spoofed e-mail address (faking someone else's e-mail address is known as "spoofing"). When unsuspecting users click the link, they're taken to an equally convincing (and equally fake) web page or pop-up window that's been set up to imitate a legitimate business. The phishing site will ask for the user's personal information, which the phisher then uses to buy things, apply for a new credit card, or otherwise steal a person's identity.

Recognizing Phishing E-mails

Spotting the imposters can be tricky since phishers go to great lengths to look like the real thing. Roll over the warning signs below.

- UNSOLICITED REQUESTS FOR PERSONAL INFORMATION.

Most businesses aren't going to ask you for your personal information out of the blue—especially not an organization such as your bank or credit card company, which should already have this information on file. If you do get a request for personal information, call the company first and make sure the request is legitimate.

- ALARMIST WARNINGS.

Phishers often attempt to get people to respond without thinking, and a message that conveys a sense of urgency, perhaps by saying that an account will be closed in 48 hours if you don't take immediate action, may cause you to do just that.

- MISTAKES.

The little things can often reveal the biggest clues. Phishers often slip up on the finer details and overlook typos, mistakes in grammar, and so on.

- ADDRESSED AS "CUSTOMER."

If your bank, for example, regularly addresses you by name in its correspondence and you get an e-mail addressed to "Dear Customer," this may be a phishing attempt.

- THE WORDS "VERIFY YOUR ACCOUNT."

A legitimate business will not ask you to send passwords, logon names, Social Security numbers, or other personally identifiable information through e-mail. Be suspicious of a message that asks for personal information no matter how authentic it looks.

- THE PHRASE "CLICK THE LINK BELOW TO GAIN ACCESS TO YOUR ACCOUNT."

HTML-formatted messages can contain links or forms that you can fill out just as you'd fill out a form on a Web site. The links that you are urged to click may contain all or part of a real company's name, but the link you see is actually taking you to a phony Web site.

PayPal Example

Can you spot where the warning is?

From: Paypal.co.uk [Alerts@Paypal.co.uk] Sent:
To: Elinor Mills
Cc:
Subject: Paypal Account Notification.

PayPal

Dec 2009

Dear users of PayPal services,

Privacy. Prevention. Protection.
PayPal

Due to upcoming changes in our Service Agreement in December 2009, you will need to submit additional details on your PayPal account. Starting in 2010 all PayPal accounts will come with complete detailed information! Identity protection matters. And PayPal works day and night to help keep your identity safe.

Identity protection matters. Get Verified!

According to the new changes in our Service Agreement, any unverified account will be deleted from the system in 72 hours after receiving this notice.

Your Account

Tips to Protect Your Account NEW!
PayPal's world class fraud investigators share 5 important

Identity Protection Highlights

New spoof tutorial
Learn how to spot and avoid fraudulent "spoof" emails and websites with PayPal's handy 5-step spoof tutorial.

Protection from Phishing

Another technique that phishers use is a Uniform Resource Locator (URL) that at first glance appears to be the name of a well-known company but is slightly altered by intentionally adding, omitting, or transposing letters. For example, the URL "www.microsoft.com" could appear instead as:

www.micosoft.com
www.mircosoft.com
www.verify-microsoft.com

To help avoid this trap, it's best to visit a Web site either by typing the URL in the address field yourself or by accessing it from your Bookmarks list. Be cautious when clicking links that claim to take you to a site.

To help prevent these phishing scams, feel free to report the e-mails by forwarding it to the following e-mail addresses:

reportphishing@antiphishing.org
spam@uce.gov

Trust your instincts. If an e-mail message looks suspicious, it probably is.

Quiz

Test your knowledge! Click one answer per question. Hit the reset button to start over.

1) What is a warning sign?

- a) Asking you to validate your account.
- b) Spelling errors.
- c) You are addressed as a "Valued Customer."
- d) All the above.

2) How do Phishers gain access to your bank account?

- a) Clicking a link.
- b) Clicking a link and giving your account information.
- c) Viewing the email.
- d) None of the above.

3) How can you protect yourself from phishing scams?

- a) Click to validate your account.
- b) Reply and tell them to stop.
- c) Delete the e-mail without clicking anything and providing information
- d) You can't protect yourself.

Type any comments here

Reset

Submit

Answers: 1d, 2b, 3c

References/Bibliography

Christensen, Brett M. "An Overview of Phishing." Latest Email Hoaxes - Current Internet Scams - Hoax-Slayer. 9 Jan. 2007. Web. 26 Mar. 2010. <http://www.hoax-slayer.com/phishing-scams-overview.shtml>.

Mills, Elinor. "Recognizing Phishing E-mails." InSecurity Complex. CNET News, 17 Nov. 2009. Web. 25 Mar. 2010. <http://news.cnet.com/8301-27080_3-10396786-245.html>.

Media

LeFever, Lee. "Phishing Scams in Plain English." Common Craft. 21 Oct. 2008. Web. 26 Mar. 2010. <http://commoncraft.com/>.

"Massive Attack Teardrop." - Sample Audio in W8 Lab Media Files

"Phishing How to Avoid Getting Hooked!" Welcome to IT Security | Information Security. 2010. Web. 26 Mar. 2010. <http://itsecurity.vermont.gov/threats/phishing>.

Pilibosian, Dave. Phishing. 2010. Photograph. IStockphoto.com. 2010. Web. 26 Mar. 2010. <http://www.istockphoto.com/>.

"Recognize Phishing Scams and Fraudulent E-mails." Microsoft Corporation. 2010. Web. 26 Mar. 2010. <http://www.microsoft.com/uk/athome/security/email/phishing.mspx>.

By: Tina Dang