DELAWARE DEPARTMENT OF TECHNOLOGY & INFORMATION April 2007 Issue

SECURITY - Now ...more than ever!

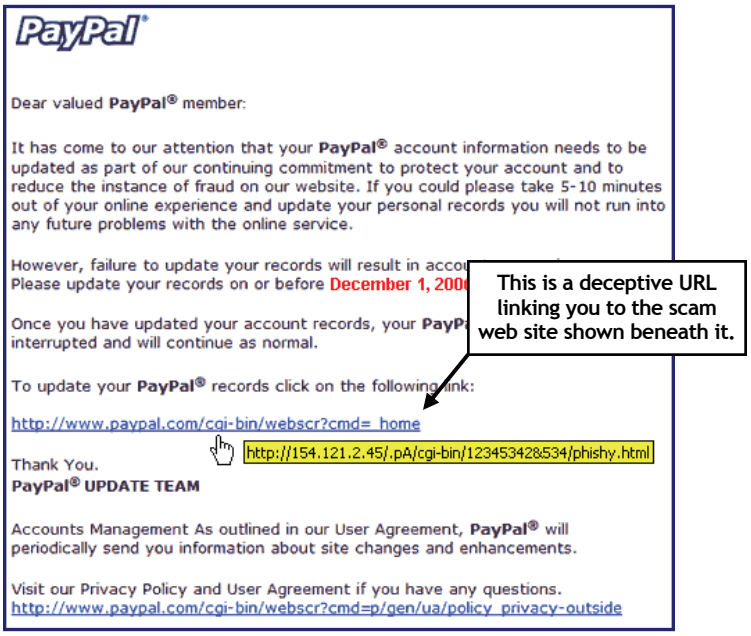
Cyber Security - Disaster Recovery - Continuity of Government

DTI eSecurity News - Don't take the bait during the next "Phishing" expedition!

Fraudulent E-mail Solicitation

"Phishing" is a computer crime that is designed to trick victims into submitting information such as Social Security numbers, credit card numbers, bank account numbers, user names and passwords, or other personal information.

The most common method for executing this kind of attack is spam e-mail. The e-mails will commonly appear to originate from a well-known, legitimate company, such as a large bank. They may contain the corporate logo and a professional sounding message in an attempt to appear official. An example of a phishing message is below:



The example above demonstrates how a seemingly authentic message is actually a fake. If you look carefully, you'll see that the link to PayPal deceptively points to a completely different URL!

The goal of these e-mails is to coax the victim into entering their information into an online form which then transmits that information to the perpetrator. These scams are becoming more sophisticated every day and harder to differentiate from legitimate e-mails.

Coming Next Month: How to Protect Your Identity

Avoid Becoming the Next Victim

1) Become educated about the security measures your web browser (such as Internet Explorer) has to offer. Most browsers offer visual cues to indicate if a site is secure such as a gold padlock *in the lower right of the bottom status bar,* and the URL will begin with "**https://**". These indicate that your computer has established a secure communication with the website you are viewing. Examples of these cues are shown below:

2) Forward these fake messages to spam@uce.gov and the impersonated institution. If you receive the message on your state e-mail address, forward it to: eSecurity@state.de.us.

3) Take notice of the upper and lower status bars. A common visual deception is used by registering a domain name such as:
www.VVachovia.com ("V"s instead of a "W")
www.Paypai.com ("i" instead of an "L")
www.Paypa1.com ('1' instead of an "L")

4) Legitimate organizations would *never* ask for your personal information in an unsolicited e-mail. If you are unsure, call the company's toll-free number to verify the e-mail.

5) If you have inadvertently submitted personal information to a phishing site, contact the real company immediately. Consider filing a police report or contacting your Attorney General's office. Also, visit these sites which have good information on what to do if you've been successfully phished:
http://www.nocpa.org/phishing/phishing-ifresponded.html
http://www.phishing.arollo.com/whattodo.html

Questions or comments?
E-mail us at
eSecurity@state.de.us