

Copyright Notice:

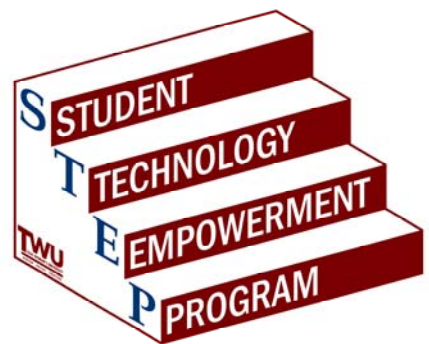
Copyright STEP 2007. This work is the intellectual property of the author. Permission is granted for this material to be shared for non-commercial, educational purposes, provided that this copyright statement appears on the reproduced materials and notice is given that the copying is by permission of the author. To disseminate otherwise or to republish requires written permission from the author.

STEP presents:

PHISHING



*Instructional Support Services
Texas Woman's University
Spring 2007*



What is Phishing?

- **Definition** - (fish'ing) (**n.**) "The act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The e-mail directs the user to visit a Web site where they are asked to update personal information, such as passwords, credit card, social security numbers, and bank account numbers that the legitimate organization already has."



Why Phish In A Sea Of People?

- Phishers want your personal information to use it for their own personal gain.
- It is simple to create a Web site that looks legitimate by mimicking another site's HTML code.
- It is cheap and easy.

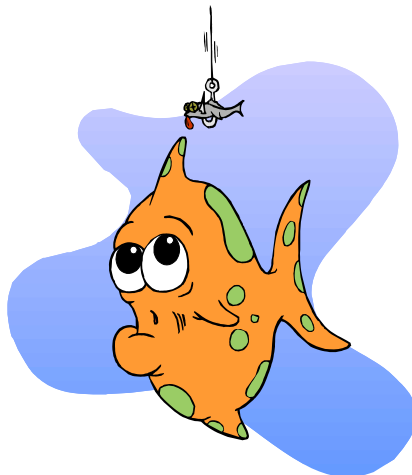
Who Is Behind Phishing??

- Scam artists who are "phishing" for some bait.
- If you have an email, you are at risk.
 - If you have made your email public, then you will be more susceptible.



Don't Let An Email Reel You In

- Phishers are not looking for every user to respond, but they are hoping for a "bite" or two.
- Many emails state that specific information is needed to update an account and others state your account may even be terminated.
- Email addresses are easily accessible on the internet.



What To Look For

- The “from” field may look like a familiar company, but it is a simple task to change the “from” information.
- Although the logos are from the company, they were likely to have been copied into the email from the actual company.
- The email also has a clickable link within the content; if you mouse over the link at the bottom left of the screen the actual Web address is shown.
- * These are just a few examples of fraudulent emails.

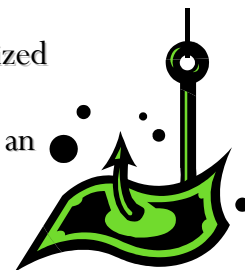


A Single Tip Is Not Good Enough

- Although all of these tips are things to look for, it is important to understand that each phisher is different.
- You should always look at two or more clues before you get reeled in and cannot get out.

How To Keep Swimming Up Stream

- Always read your credit card statements in the mail to look for unauthorized charges.
- If you are uncertain about the information, contact the company through an address or telephone number you know to be genuine.
- Be cautious when opening an attachment or downloading email files.
- Use anti-virus software or a firewall (keep them updated).
- If you unknowingly supplied personal or financial information, contact your bank and credit card company immediately.
- Suspicious e-mail can be forwarded to uce@ftc.gov. Complaints should be filed with the state Attorney General's office or through the Federal Trade Commission at www.ftc.gov or 1-800-FTC-HELP.



Spear Phishing

- This is the newest addition to the phishing scam that is highly targeted.
- Definition- “A type of phishing that focuses on a single user or department within a single organization. The Phish appears to be legitimately addressed from someone within that company, in a position of trust, and request information such as login IDs and passwords.”
- The email will appear to be from a trusted person within a company, usually the human resources or technical support.
- Passwords, usernames and other personal information are usually asked for.
- When the hackers receive this information, they can log into the entire company’s system.
- If you click the link within the email, spyware could spread across the entire network.

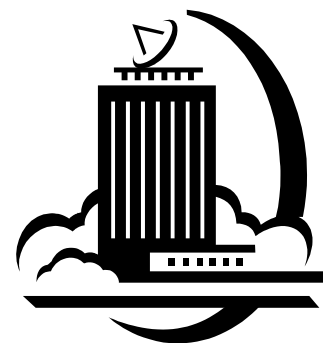


How To Avoid Getting Hooked

- NEVER in any circumstances give out personal information over email.
- At the first sign of a suspicious email, personally get in touch with the person or organization the email is supposedly from.
- NEVER click on links from an email that is asking for personal information.
- Do not be hesitant to report a suspicious email to the company that the email appears to be from.
- Microsoft has a Phishing Filter; for more information visit the Microsoft Web site.

Companies That Have Been Affected

- Banks
 - Wells Fargo, Citi Bank
- Online Accounts
 - PayPal
- Personal Accounts
 - People in other countries asking for money to help



Damage Caused

- Identity theft could lead to:
 - Unauthorized bank transfers.
 - Fake accounts and bad credit.
 - Not being able to access your own account.
 - Obtaining personal information by accessing public records.
 - Financial loss.



Tall Tails

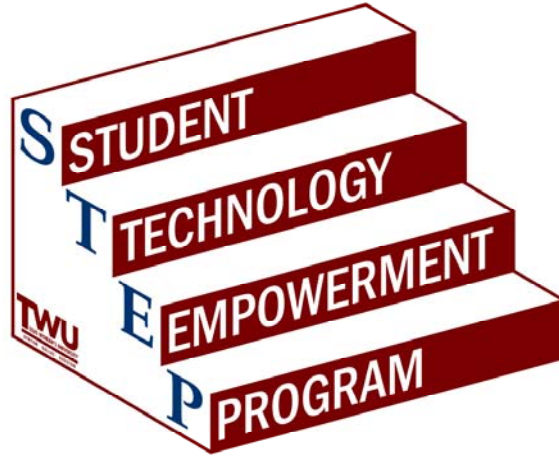
- Myth- A secure, encrypted web page is a valid page.
 - Truth- Never rely solely on the web address. It is possible for any site to be a phishing site.
- Myth- The address bar always shows the correct address.
 - Truth- Vulnerabilities in the browser may allow phishers to spoof information in the address bar.
- Myth- It is safe to log in to a site once you know it is legitimate.
 - Truth- An intelligent scam artist could use the original company's forms to redirect you to an illegitimate site as soon as you "login".



References

- http://www.microsoft.com/athome/security/email/spear_phishing.mspix
- <http://www.webopedia.com/TERM/p/phishing.html>
- <http://www.webopedia.com/DidYouKnow/Internet/2005/phishing.asp>
- <http://www.ftc.gov/bcp/conline/pubs/alerts/phishingalrt.htm>
- <http://en.wikipedia.org/wiki/Phishing>
- <http://www.hexview.com/sdp/node/24>
- <http://www.pcworld.com/article/id,118489-page,1/article.html>

Thank You For Coming!



Phone: 940-898-3288

Fax: 940-898-3499

E-mail: STEP@twu.edu

Web: <https://portal.twu.edu/step>