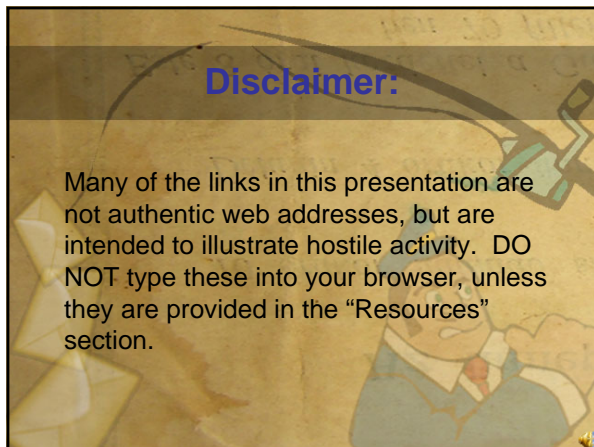


- Definition of Phishing
- State of Phishing Today
- Recognizing Phishing/Phishing Tricks
- Examples
- Best Practices
- What to do if you get "hooked"
- Summary



Many of the links in this presentation are not authentic web addresses, but are intended to illustrate hostile activity. DO NOT type these into your browser, unless they are provided in the "Resources" section.



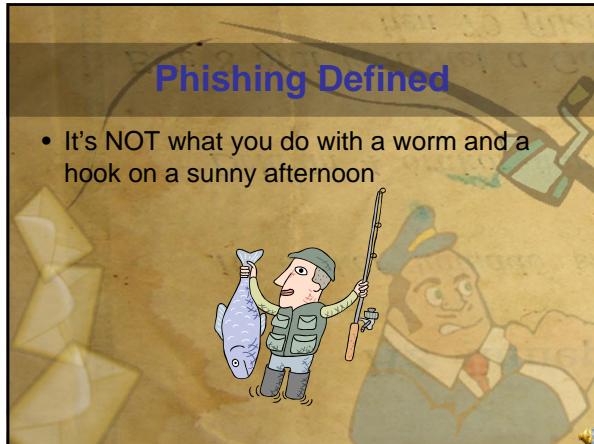
Definition

- Web Address
 - Located in the top portion of the screen
 - Begins with http or https
 - The unique address of the web page

Web Address Example

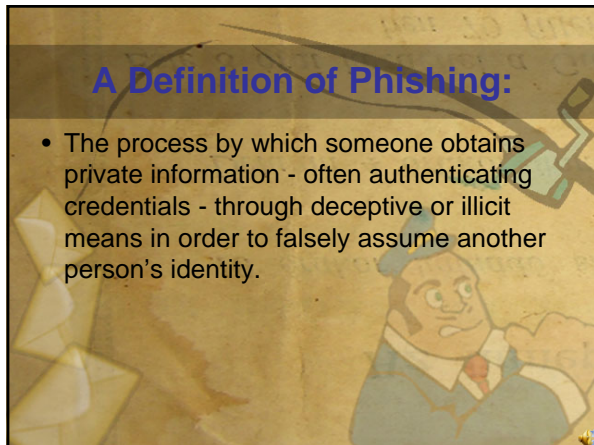
Phishing Defined

- It's NOT what you do with a worm and a hook on a sunny afternoon



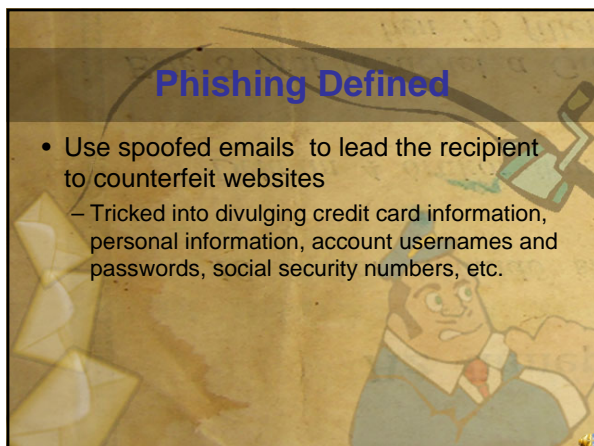
A Definition of Phishing:

- The process by which someone obtains private information - often authenticating credentials - through deceptive or illicit means in order to falsely assume another person's identity.



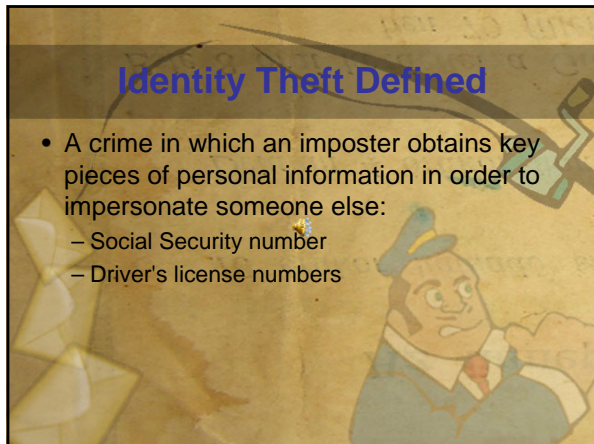
Phishing Defined

- Use spoofed emails to lead the recipient to counterfeit websites
 - Tricked into divulging credit card information, personal information, account usernames and passwords, social security numbers, etc.



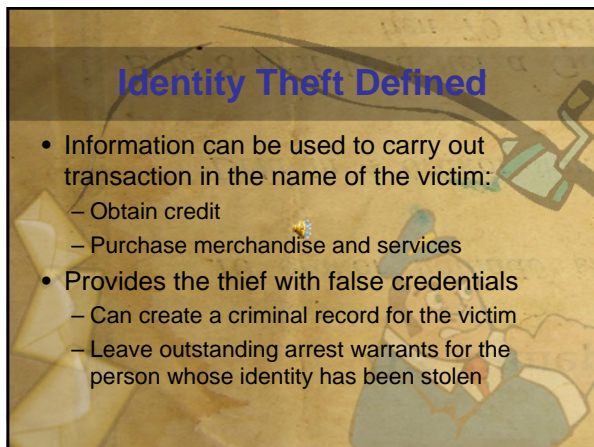
Identity Theft Defined

- A crime in which an imposter obtains key pieces of personal information in order to impersonate someone else:
 - Social Security number
 - Driver's license numbers



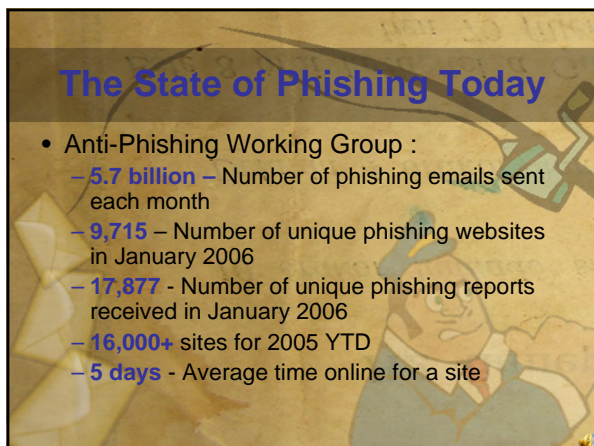
Identity Theft Defined

- Information can be used to carry out transaction in the name of the victim:
 - Obtain credit
 - Purchase merchandise and services
- Provides the thief with false credentials
 - Can create a criminal record for the victim
 - Leave outstanding arrest warrants for the person whose identity has been stolen



The State of Phishing Today

- Anti-Phishing Working Group :
 - **5.7 billion** – Number of phishing emails sent each month
 - **9,715** – Number of unique phishing websites in January 2006
 - **17,877** - Number of unique phishing reports received in January 2006
 - **16,000+** sites for 2005 YTD
 - **5 days** - Average time online for a site



Identity Theft Statistics

- From FTC Identity Theft Survey Report 2003:
 - **9.9 million** – Number of victims
 - **\$47.6 billion** – Loss to businesses
 - **\$5 billion** – Total loss to victims
 - **2 – 10,000 hours** – Range of time spent by victims on resolving the problem (Average was **600 hours**)

The State of Phishing Today

- “Why Phishing Works” study found:
 - People do not know how to scrutinize web addresses
 - Even when presented with a choice between a valid and a hoax site, the hoax was selected 40% of the time
- Spam VS. Phishing
 - **Spam** – Selling
 - **Phishing** - Stealing

Recognizing Phishing

- Look for the following three components:
 - **Build credibility** (sounds good)
 - Spoof a real company
 - You may or may not be a member or have an account
 - **Create a reason to act**
 - Urgency, plausible premise, requires quick response
 - **A call to action**
 - Click a link or button
 - Subtle changes to web address
 - Actual web address with changed link properties
 - Not going where you think you are going!

Recognizing Phishing

- Exercise caution when:
 - Notified of “internal accounting errors”, requesting your cooperation
 - Warnings of your account being closed if action is not taken
 - Requests to update your account or profile
 - Apparent notices from your ISP informing you of problems generated by your PC

For Example

PayPal The way to send and receive money online.

Security Message

Dear PayPal Customer,

In accordance with our major database relocation, we are currently having major adjustments and updates of user accounts to verify that the information you have provided with us during the sign-up process are true and correct. However, we have noticed some discrepancies regarding your account at PayPal. Possible causes are inaccurate contact information and invalid login process.

We require you to complete an account verification procedure as part of our security measure.

You must click the link to complete the process.

[Click here to confirm your account](#)

Please Note

Unable to do so may result to abnormal account behavior during transactions. We thank you for your prompt attention to this matter. Please understand that this is a security measure extended to help protect you and your account.

We apologize for any inconvenience.

Sincerely,
 PayPal Account Review Department
 PayPal Email ID: PPS60

PayPal The way to send and receive money online.

Security Message

Dear PayPal Customer,

In accordance with our major database relocation, we are currently having major adjustments and updates of user accounts to verify that the **information** you have provided with us during the sign-up process are true and correct. However, we have noticed some discrepancies regarding your account at PayPal. Possible causes are inaccurate contact information and invalid login process.

We require you to complete an account verification procedure as part of our security measure.

You must click the link to complete the process.

[Click here to confirm your account](#)

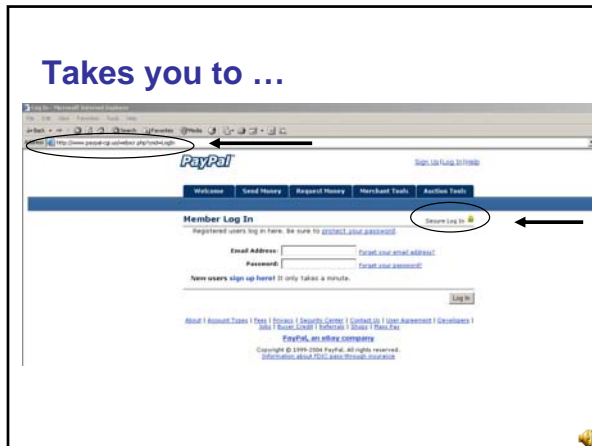
Please Note

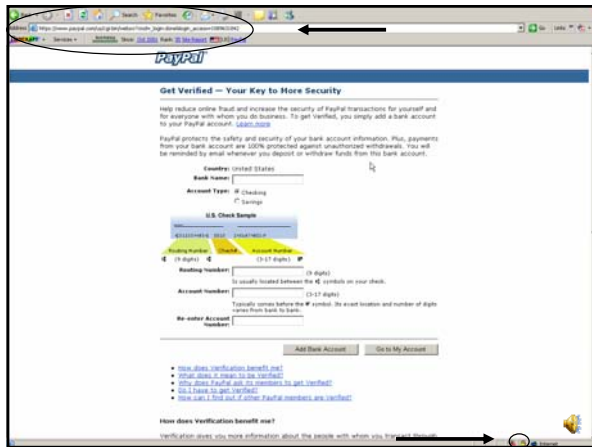
Unable to do so may result to abnormal account behavior during transactions. We thank you for your prompt attention to this matter. Please understand that this is a security measure extended to help protect you and your account.

We apologize for any inconvenience.




Sincerely,
 PayPal Account Review Department
 PayPal Email ID: PPS60

Takes you to ...





Secure Site

- **Https**
 - **Internet Explorer** Lock icon: 
 - Displayed in lower right
 - **Mozilla FireFox** Lock icon: 
 - Displayed in lower left
 - **Netscape** Lock icon: 
 - Displayed in lower left

Recognizing Phishing

- The actual domain comes JUST BEFORE the domain suffix
 - Example: www.uakron.edu
 - Uakron = domain
 - .edu = suffix
 - Suffixes:
 - .com = Commercial business
 - .edu = Educational institutions
 - .gov = Government
 - .org = Non-Profit organizations
 - .mil = Military
 - .net = Network organizations

Recognizing Phishing

- Look for the following (examples of fraudulent links):
 - <http://eBay.signon.com>
 - <http://BanesAndNoble.com>
 - www.ebay.com@xyz.com
 - www.xyz.com/paypal-login.html
- Anything after a 'slash' is a subdirectory of the website

Phishing Tricks

- Credible-looking web address
 - http://81.109.44.105/ebay/account_update/now.php
- The @ sign
 - Uses everything to the right of the @
 - Everything to the left of the @ is forgotten
 - <http://www.usbank.com/update.pl@81.109.43.103/usb/upd.pl>
- Long status line
 - Web address is so long it cannot be completely displayed in the status bar (combine with @ sign)

