How to Avoid Phishing Scams

The number and sophistication of phishing scams sent out to consumers is continuing to increase dramatically. While online banking and e-commerce is very safe, as a general rule you should be careful about giving out your personal financial information over the Internet. The **Anti-Phishing Working Group** has compiled a list of recommendations below that you can use to avoid becoming a victim of these scams.

- Be suspicious of any email with urgent requests for personal financial information
    - unless the email is digitally signed, you can't be sure it wasn't forged or 'spoofed'
    - phishers typically include upsetting or exciting (but false) statements in their emails to get people to react immediately
    - they typically ask for information such as usernames, passwords, credit card numbers, social security numbers, date of birth, etc.
    - phisher emails are typically NOT personalized, but they can be. Valid messages from your bank or e-commerce company generally are personalized, but always call to check if you are unsure
- Don't use the links in an email, instant message, or chat to get to any web page if you suspect the message might not be authentic or you don't know the sender or user's handle
    - instead, call the company on the telephone, or log onto the website directly by typing in the Web address in your browser
- Avoid filling out forms in email messages that ask for personal financial information
    - you should only communicate information such as credit card numbers or account information via a secure website or the telephone
- Always ensure that you're using a secure website when submitting credit card or other sensitive information via your Web browser
    - Phishers are now able to 'spoof,' or forge BOTH the "https://" that you normally see when you're on a secure Web server AND a legitimate-looking address. You may even see both in the link of a scam email. Again, make it a habit to enter the address of any banking, shopping, auction, or financial transaction website yourself and not depend on displayed links.
    - Phishers may also forge the yellow lock you would normally see near the bottom of your screen on a secure site. The lock has usually been considered as another indicator that you are on a 'safe' site. The lock, when double-clicked, displays the security certificate for the site. If you get any warnings displayed that the address of the site you have displayed does NOT match the certificate, do not continue.
- Remember not all scam sites will try to show the "https://" and/or the security lock. Get in the habit of looking at the address line, too. Were you directed to PayPal? Does the address line display something different like "http://www.gotyouscammed.com/paypal/login.htm?" Be aware of where you are going.
- Be cautious about opening any attachment or downloading any files from emails you receive, regardless of who sent them. These files can contain viruses or other software that can weaken your computer's security.
- Consider installing a Web browser tool bar to help protect you from known fraudulent websites. These toolbars match where you are going with lists of known phisher Web sites and will alert you.
    - The newer version of Internet Explorer version 7 includes this tool bar as does FireFox version 2
    - EarthLink ScamBlocker is part of a browser toolbar that is free to all Internet users - download at http://www.earthlink.net/earthlinktoolbar
- Regularly log into your online accounts
    - don't leave it for as long as a month before you check each account

- Regularly check your bank, credit and debit card statements to ensure that all transactions are legitimate
    - if anything is suspicious or you don't recognize the transaction, contact your bank and all card issuers
- Ensure that your browser is up to date and security patches applied
- Always report "phishing" or “spoofed” e-mails to the following groups:
    - forward the email to reportphishing@antiphishing.org
    - forward the email to the Federal Trade Commission at spam@uce.gov
    - forward the email to the "abuse" email address at the company that is being spoofed (e.g. "spoof@ebay.com")
    - when forwarding spoofed messages, always include the entire original email with its original header information intact
    - notify The Internet Crime Complaint Center of the FBI by filing a complaint on their website: www.ic3.gov/

Information obtained from **http://www.antiphishing.org/consumer_recs.html**