

How to Avoid Phishing Scams

The following was taken from <http://www.antiphishing.org>

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, etc.
 - phisher emails are typically NOT personalized, while valid messages from your bank or e-commerce company generally are
- Don't use the links in an email to get to any web page, if you suspect the message might not be authentic
 - 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
 - to make sure you're on a secure Web server, check the beginning of the Web address in your browsers address bar - it should be "https://" rather than just "http://"

- Consider installing a Web browser tool bar to help protect you from known phishing fraud websites
 - EarthLink ScamBlocker is part of a free browser toolbar that alerts you before you visit a page that's on Earthlink's list of known fraudulent phisher Web sites.
 - Its 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, contact your bank and all card issuers
- Ensure that your browser is up to date and security patches applied
 - in particular, people who use the Microsoft Internet Explorer browser should immediately go to the Microsoft Security home page -- <http://www.microsoft.com/security/> -- to download a special patch relating to certain phishing schemes
- Always report "phishing" or "spoofed" e-mails to the following groups:
 - forward the email to the Federal Trade Commission at uce@ftc.gov
 - forward the email to reportphishing@antiphishing.com
 - 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 Fraud Complaint Center of the FBI by filing a complaint on their website: www.ifccfbi.gov/

For more information, check some of the following sources:

1. <http://www.antiphishing.org>.
2. For more information about how to protect yourself, see our Fact Sheet 17a Identity Theft: What to do if It Happens to You at <http://www.privacyrights.org/fs/fs17a.htm>.
3. Read the information and tips put out by the Federal Trade Commission about phishing at <http://www.ftc.gov/bcp/conline/pubs/alerts/phishingalrt.htm>.
4. Read the Department of Justice's recent whitepaper "Special Report on Phishing" at http://www.antiphishing.org/DOJ_Special_Report_On_Phishing_Mar04.pdf