

Outlook Express
PHISHING

© Darry D Eggleston, 813.677.2871, DarryD@darryd.com



One of the most challenging threats to your e-mail is something called “phishing.”

Phishing, pronounced “fishing,” is a scam to steal valuable information such as credit cards, social security numbers, user IDs and passwords. Also known as “brand spoofing,” an official-looking e-mail is sent to potential victims pretending to be from their ISP, retail store, etc., and that due to internal accounting errors or some other pretext, certain information must be updated to continue the service.

A link in the e-mail message directs the user to a Webpage that asks for financial information. The page looks genuine, because it is easy to fake a valid Web site. Any HTML page on the Web can be copied and modified to suit the phishing scheme. Such e-mails can be sent to people on selected lists or to any list, expecting that some percentage of the recipients will actually have an account with the real organization. The term comes from “fishing,” where bait is used to catch a fish. In phishing, e-mail is the bait.

Here is consumer advice from the Federal Trade Commission (FTC): “How to Avoid Phishing Scams” shared by the Florida Consumer Network

Ever get an e-mail that looks like its from a bank or financial institution? These scams usually will request you confirm (enter) your financial information like credit card numbers and pins. Don’t do it. Your bank already knows this information and won’t ask you for it. Its called a “phishing” scam.

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.

1. Be suspicious of any e-mail with urgent requests for personal financial information —

- unless the e-mail 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 e-mails to get people to react immediately

- they typically ask for information such as usernames, passwords, credit card numbers, social security numbers, etc.

- phisher e-mails are typically NOT personalized, while valid messages from your bank or e-commerce company generally are

2. Don't use the links in an e-mail to get to any Webpage, 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

3. Avoid filling out forms in e-mail 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

4. 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 browser's address bar — it should be "https://" rather than just "http://"

5. Consider installing a Web browser ToolBar 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. It's free to all Internet users — download at <http://www.earthlink.net/earthlinkToolBar>

6. Regularly log into your online accounts. Don't leave it for as long as a month before you check each account

7. 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.

8. Ensure that your browser is up-to-date and security patches applied. In particular, people who use the Microsoft Internet Explorer browser should go to the Microsoft Security home page — <http://www.microsoft.com/security/> — to download a special patch relating to certain phishing schemes
9. Always report “phishing” or “spoofed” e-mails to these groups:
 - forward the e-mail to reportphishing@antiphishing.com
 - forward the e-mail to the Federal Trade Commission at spam@uce.gov
 - forward the e-mail to the “abuse” e-mail address at the company that is being spoofed (e.g. “spoofer@ebay.com”)
10. When forwarding spoofed messages, always include the entire original e-mail with its original header information intact.
11. Notify the Internet Fraud Complaint Center of the FBI by filing a complaint on their Website: www.ifccfbi.gov/
12. Read “Identity Theft: What to do if It Happens to You” at <http://www.privacyrights.org/fs/fs17a.htm>
13. Read the info and tips put out by the Federal Trade Commission about phishing at <http://www.ftc.gov/bcp/online/pubs/alerts/phishingalrt.htm>
14. Read the Department of Justice’s recent whitepaper “Special Report on Phishing” at http://www.antiphishing.org/DOJ_Special_Report_On_Phishing_Mar04.PDF.