# The Email Phishing Fraud

Is Anyone Phishing You? That is a new word. (It is pronounced "fishing.") It is the name of a new illegal practice. Criminals send out emails that appear to be from legitimate companies. The emails instruct the receiver to go to, what appears to be a legitimate website, where he is asked for information such as credit card numbers, user names and passwords, Social Security numbers, etc. The information is later used for a variety of illegal activities.

Each such website only remains online for an average of 2.25 days; then it is removed. Various phishing techniques have been around since February.

I have here a complete *"Anti-Phishing Working Group"* (APWG) paper issued by a major U.S. banking coalition. Hundreds of thousands of Americans are being swindled.

"A consumer receives a forged email that pretends to be from a bank. The email claims that the recipient must verify his email address; and a web link is included. When clicked, the user's browser is opened; and he is taken to a web page with an email verification form. The web link is HTML; and the displayed text appears to be the real bank's site."

When you go to that website, it appears exactly like the bank's official site!

"Because the fake address bar remains installed [on your computer] even after you leave the phisher's site, there is a possibility that the phisher could use this to secretly track every web site that you visit, buy from, or sell to."

Here is data from another APWG paper:

"Consumer Advice - 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.

"Be suspicious of any email with urgent requests for personal financial information.

"Don't use the links in an email to any web page, if you suspect the message might not be authentic. Instead, call the company on the telephone or log on to 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 browser's 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 is on Earthlink's list of known fraudulent phisher websites. [But the other report said the websites change every 2.25 days!] It is free, and can be downloaded at

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 supicious, contact your bank and all card issuers.

"Make sure your browser is up to date and security patches applied.

"Ensure that your browser is up to date and security patches applied. Especially if you use Microsoft Internet Explorer browser, go to their home page and download a special patch relating to certain phishing schemes: microsoft.com/security/"

"Report 'phishing' or 'spoofed' emails to the following groups:

Forward the email to:

reportphishing@antiphishing.com

Also forward the email to the Federal Trade Commission (FTC) at: spam@uce.gov

Forward the email to the "abuse" email address at the company that is being spoofed. (One example is 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: ifccfbi.gov

For more information:

APWG fact sheet: privacyrights.org/fs/17a.htm

Federal Trade Commission information sheet:

ftc.gov/bcp/conline/pubs/alerts/phishingalrt.htm

Department of Justice recent special report:

antiphishing.org/DOJ_Special_Report_On_Phishing_Mar04.pdf

Another device is to send you an email with the note, "If you do not want to keep receiving these emails, click here."

Doing so can cause you trouble.