FTC Consumer Alert

Federal Trade Commission ■ Bureau of Consumer Protection ■ Office of Consumer & Business Education

How Not to Get Hooked by a 'Phishing' Scam

"We suspect an unauthorized transaction on your account.
To ensure that your account is not compromised,
please click the link below and confirm your identity."

"During our regular verification of accounts, we couldn't verify your information.
Please click here to update and verify your information."

Have you received email with a similar message? It's a scam called "phishing" — and it involves Internet fraudsters who send spam or pop-up messages to lure personal information (credit card numbers, bank account information, Social Security number, passwords, or other sensitive information) from unsuspecting victims.

According to the Federal Trade Commission (FTC), the nation's consumer protection agency, phishers send an email or pop-up message that claims to be from a business or organization that you may deal with — for example, an Internet service provider (ISP), bank, online payment service, or even a government agency. The message may ask you to "update," "validate," or "confirm" your account information. Some phishing emails threaten a dire consequence if you don't respond. The messages direct you to a website that looks just like a legitimate organization's site. But it isn't. It's a bogus site whose sole purpose is to trick you into divulging your personal information so the operators can steal your identity and run up bills or commit crimes in your name.

The FTC suggests these tips to help you avoid getting hooked by a phishing scam:

- **If you get an email or pop-up message that asks for personal or financial information, do not reply. And don't click on the link in the message, either.** Legitimate companies don't ask for this information via email. If you are concerned about your account, contact the organization mentioned in the email using a telephone number you know to be genuine, or open a new Internet browser session and type in the company's correct Web address yourself. In any case, don't cut and paste the link from the message into your Internet browser — phishers can make links look like they go to one place, but that actually send you to a different site.

- **Area codes can mislead.** Some scammers send an email that appears to be from a legitimate business and ask you to call a phone number to update your account or access a "refund." Because they use Voice Over Internet Protocol technology, the area code you call does not reflect where the scammers really are. If you need to reach an organization you do business with, call the number on your financial statements or on the back of your credit card. In any case, delete random emails that ask you to confirm or divulge your financial information.

AUTHENTICATED U.S. GOVERNMENT INFORMATION GPO

- **Use anti-virus and anti-spyware software, as well as a firewall, and update them all regularly.** Some phishing emails contain software that can harm your computer or track your activities on the Internet without your knowledge.

  Anti-virus software and a firewall can protect you from inadvertently accepting such unwanted files. Anti-virus software scans incoming communications for troublesome files. Look for anti-virus software that recognizes current viruses as well as older ones; that can effectively reverse the damage; and that updates automatically.

  A firewall helps make you invisible on the Internet and blocks all communications from unauthorized sources. It's especially important to run a firewall if you have a broadband connection. Operating systems (like Windows or Linux) or browsers (like Internet Explorer or Netscape) also may offer free software "patches" to close holes in the system that hackers or phishers could exploit.

- **Don't email personal or financial information.** Email is not a secure method of transmitting personal information. If you initiate a transaction and want to provide your personal or financial information through an organization's website, look for indicators that the site is secure, like a lock icon on the browser's status bar or a URL for a website that begins "https:" (the "s" stands for "secure"). Unfortunately, no indicator is foolproof; some phishers have forged security icons.

- **Review credit card and bank account statements as soon as you receive them** to check for unauthorized charges. If your statement is late by more than a couple of days, call your credit card company or bank to confirm your billing address and account balances.

- **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.

- **Forward spam that is phishing for information** to spam@uce.gov and to the company, bank, or organization impersonated in the phishing email. Most organizations have information on their websites about where to report problems.

- **If you believe you've been scammed, file your complaint at ftc.gov**, and then visit the FTC's Identity Theft website at www.consumer.gov/idtheft. Victims of phishing can become victims of identity theft. While you can't entirely control whether you will become a victim of identity theft, you can take some steps to minimize your risk. If an identity thief is opening credit accounts in your name, these new accounts are likely to show up on your credit report. You may catch an incident early if you order a free copy of your credit report periodically from any of the three major credit bureaus. See www.annualcreditreport.com for details on ordering a free annual credit report.

  You can learn other ways to avoid email scams and deal with deceptive spam at ftc.gov/spam.

The FTC works for the consumer to prevent fraudulent, deceptive, and unfair business practices in the marketplace and to provide information to help consumers spot, stop, and avoid them.

To file a complaint or to get free information on consumer issues, visit ftc.gov or call toll-free, 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261. The FTC enters Internet, telemarketing, identity theft, and other fraud-related complaints into Consumer Sentinel, a secure, online database available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.

FEDERAL TRADE COMMISSION	ftc.gov
1-877-FTC-HELP	FOR THE CONSUMER

October 2006