
FTC Consumer Alert

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

How Not to Get Hooked by a 'Phishing' Scam

Internet scammers casting about for people's financial information have a new way to lure unsuspecting victims: They go "phishing."

Phishing is a high-tech scam that uses spam or pop-up messages to deceive you into disclosing your credit card numbers, bank account information, Social Security number, passwords, or other sensitive information.

According to the Federal Trade Commission (FTC), phishers send an email or pop-up message that claims to be from a business or organization that you deal with – for example, your Internet service provider (ISP), bank, online payment service, or even a government agency. The message usually says that you need to "update" or "validate" your account information. It might threaten some dire consequence if you don't respond. The message directs you to a Web site that looks just like a legitimate organization's site, but it isn't. The purpose of the bogus site? 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, the nation's consumer protection agency, 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 or click on the link in the message**. Legitimate companies don't ask for this information via email. If you are concerned about your account, contact the organization 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. In any case, don't cut and paste the link in the message.
 - **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 Web site, 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 determine whether there are any 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.
 - **Use anti-virus software and keep it up to date**. 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. Finally, your operating system (like Windows or Linux) may offer free software "patches" to close holes in the system that hackers or phishers could exploit.

- **Be cautious about opening any attachment or downloading any files from emails you receive**, regardless of who sent them.
- **Report suspicious activity to the FTC.** If you get spam that is phishing for information, forward it to spam@uce.gov. If you believe you've been scammed, file your complaint at www.ftc.gov, and then visit the FTC's Identity Theft Web site at www.consumer.gov/idtheft to learn how to minimize your risk of damage from ID theft. Visit www.ftc.gov/spam to learn other ways to avoid email scams and deal with deceptive 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 www.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.



June 2004
