FTC Consumer Alert

Federal Trade Commission ■ Bureau of Consumer Protection ■ Office of Consumer and 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, also called "carding," is a high-tech scam that uses spam to deceive consumers into disclosing their credit card numbers, bank account information, Social Security numbers, passwords, and other sensitive information.

According to the Federal Trade Commission (FTC), the emails pretend to be from businesses the potential victims deal with — for example, their Internet service provider (ISP), online payment service or bank. The fraudsters tell recipients that they need to "update" or "validate" their billing information to keep their accounts active, and direct them to a "look-alike" Web site of the legitimate business, further tricking consumers into thinking they are responding to a bona fide request. Unknowingly, consumers submit their financial information — not to the businesses — but the scammers, who use it to order goods and services and obtain credit.

To avoid getting caught by one of these scams, the FTC, the nation's consumer protection agency, offers this guidance:

- If you get an email that warns you, with little or no notice, that an account of yours will be shut down unless you reconfirm your billing information, do not reply or click on the link in the email. Instead, contact the company cited in the email using a telephone number or Web site address you **know** to be genuine.
- Avoid emailing personal and financial information. Before submitting financial information through a Web site, look for the "lock" icon on the browser's status bar. It signals that your information is secure during transmission.
- 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.
- Report suspicious activity to the FTC. Send the actual spam to uce@ftc.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 (www.ftc.gov/idtheft) to learn how to minimize your risk of damage from identity theft.
- Visit www.ftc.gov/spam to learn other ways to avoid email scams and deal with deceptive spam.

The Federal Trade Commission 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.