

## **How to Protect Yourself: Phishing**

*Source: The Florida Attorney General*

Phishing is the term coined by Internet scammers who imitate legitimate companies in e-mails to entice people to share user names, passwords, account information or credit-card numbers.

The term Phishing comes from the fact that Internet scammers are using increasingly sophisticated lures as they "fish" for users' private information. The most common ploy is to copy the look and feel of a web page from a major site and use that design to set up a nearly identical page that appears to be part of the company's site.

### **Don't Take the Bait from 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) and other responsible company websites, the emails pretend to be from businesses the potential victims already have a relationship with. These include their Internet service provider (ISP), online payment service or bank. The "phisher" tells 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. Other related crimes include credit card fraud or theft and identity theft.

There are several steps you can take to make sure you never fall for one of these scams:

- 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.
- Always ensure that you're using a secure server when submitting credit card information. To make sure you're using a secure server, check the beginning of the web address in your browsers address bar - it should be https:// rather than just http://.
- Contact your bank or Credit Card Company if you think you may have replied to a fraudulent E-Mail with sensitive personal information.
- Report suspicious activity to the FTC. Send the actual spam to spam@uce.gov. If you believe you've been scammed, file your complaint at

- [www.ftc.gov](http://www.ftc.gov), and then visit the Attorney General's identity Theft Web site at <http://myfloridalegal.com/identitytheft> for information on how to protect yourself from identity theft.
- Finally Microsoft has recently created a security update for Internet Explorer that will help you avoid Phishing scams. It removes a vulnerability that could allow an attacker to mis-represent the location of a Web page in the Address bar of an Internet Explorer window. We strongly urge you apply this patch if your computer has Internet Explorer installed (even if you do not use Internet Explorer as your primary web browser). To install this security update, please visit: <http://www.microsoft.com/technet/security/Bulletin/MS04-004.asp> for additional information.

For additional information on SPAM Enforcement please visit our [SPAM](#) page.