

Ask Your Banker...

# Phishing Scams



American Bankers Association

## Don't Get Phished

Internet "phishing" scams are one of the fastest-growing frauds today. Phishing expeditions can range from an elaborate Web site with fake graphics and logos to a simple text e-mail offering a great mortgage rate. Both are designed for one purpose: to collect e-mail recipients' personal financial details, such as credit card numbers, bank account usernames and passwords.

By hijacking the trusted brands of banks, online retailers, credit card companies and even government agencies, fraudsters are able to trick some consumers into handing over their personal financial information.

## How to Protect Yourself

- Never respond to an unsolicited e-mail that asks for detailed financial information.
- When submitting financial information to a Web site, look for the padlock icon in your browser, normally near the Internet address, and make sure the address begins with "https."
- If you have not already done so, sign up for online banking. Check your credit card and bank account transactions and balances online regularly and report discrepancies immediately.
- Use anti-virus and anti-spyware software, as well as a firewall, and update them all regularly. Some phishing e-mails contain software that can harm your computer or track your activities on the Internet without your knowledge.

© 2009 The American Bankers Association. All rights reserved.

- Contact the Internet Crime Complaint Center at [www.ic3.gov](http://www.ic3.gov)—a partnership between the FBI and the National White Collar Crime Center—if you think you have received a phishing e-mail or have been directed to a suspicious Web site.

## "Stop, Look and Call"

The Department of Justice advises consumers to "stop, look and call" if they receive a suspicious e-mail.

- **Stop.** Resist that impulse to click or respond immediately. No matter how upsetting or exciting the statements in the e-mail may be, take the time to check out the information more closely.
- **Look.** Read the text of the e-mail and ask yourself if the claims make sense, especially if personal financial information is being requested.
- **Call.** Telephone the organization identified, using a number that you know to be legitimate (taken from a phone book, for example).

## If You've Become the Victim of a Phishing Scam

If you believe you've given out sensitive financial information to a fraudster, you should:

- Report the incident to your financial institution as quickly as possible.

- Contact these three major credit bureaus and request that a fraud alert be placed on your credit report: Equifax, 1-800-525-6285; Experian, 1-888-397-3742; and TransUnion, 1-800-680-7289.
- File a complaint with the Federal Trade Commission at [www.ftc.gov](http://www.ftc.gov) or 1-877-382-4357, or the Anti-Phishing Working Group at [www.antiphishing.org](http://www.antiphishing.org).

## **Remember:**

**Your bank will never ask for or send you personal financial information by e-mail. Don't get hooked by a phishing scam!**

Product ID-3005749