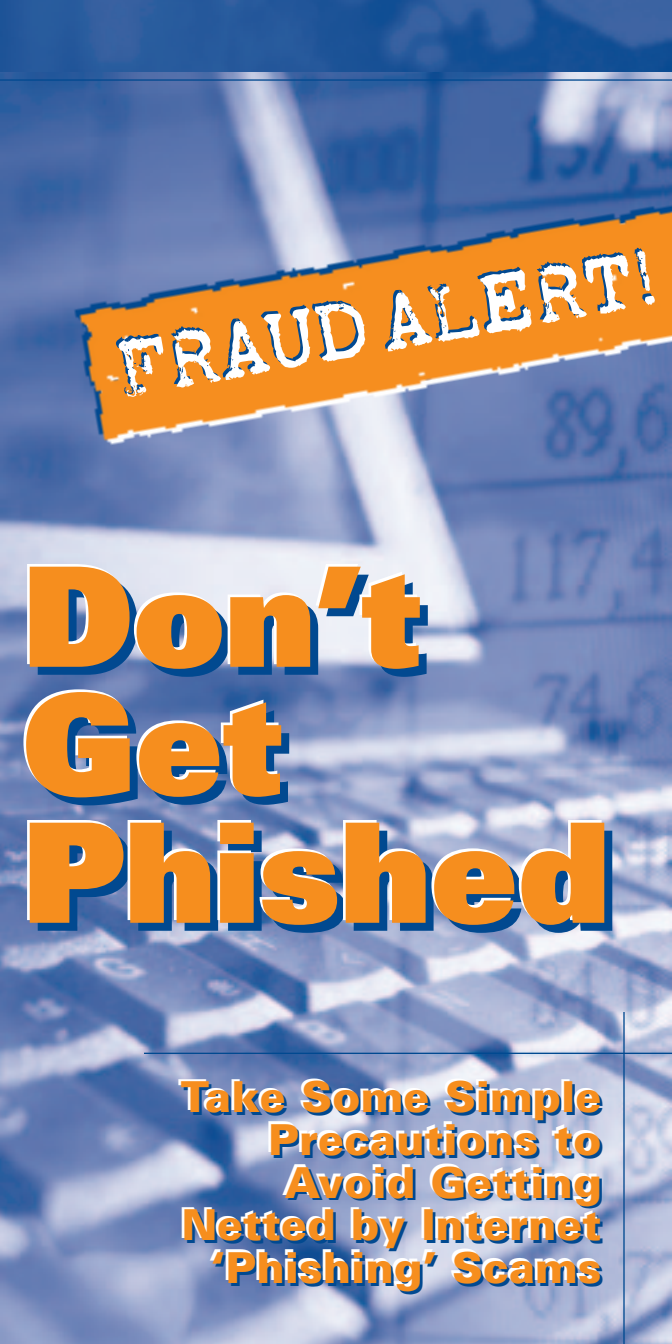

Don't Get Phished

Take Some Simple Precautions to Avoid Getting Netted by Internet 'Phishing' Scams

Protecting Yourself Against E-mail Fraud

Internet "phishing" scams are one of the fastest-growing frauds today. Phishing typically involves a bogus e-mail message that uses legitimate materials, such as a company's Web site graphics and logos, in an attempt to entice e-mail recipients to provide personal financial details, such as credit card and Social Security numbers.

Financial institutions, government agencies, retailers, credit card companies and many other organizations have seen their Web site graphics, including corporate logos and other materials, "borrowed" by fraudsters intent on tricking consumers into divulging personal financial information by responding to an official-looking, but entirely bogus, e-mail. Like many cons and scams, phishing preys on the unwary. Here's how you can keep your guard up, and help fight back against this form of fraud.

TAKE SOME SIMPLE PRECAUTIONS.

- ✔ Never respond to an unsolicited e-mail that asks for detailed financial information. Know whom you are dealing with.
- ✔ Report anything suspicious to the proper authorities. Alert the company or government agency identified in the suspect e-mail through a Web address or telephone number that you know is legitimate.

- You can also contact the Internet Crime Complaint Center at **www.ifccfbi.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 "phishy-looking" Web site.

"STOP, LOOK AND CALL"

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

- **Stop.** Resist the urge to immediately respond to a suspicious e-mail—and to provide the information requested—despite urgent or exaggerated claims.
- **Look.** Read the text of the e-mail several times and ask yourself why the information requested would really be needed.
- **Call.** Telephone the organization identified, using a number that you know to be legitimate.

IF YOU'VE BEEN "PHISHED..."

If you believe that you have provided sensitive financial information about yourself through a phishing scam, you should:

- Immediately contact your financial institution.
- Contact the three major credit bureaus and request that a fraud alert be placed on your credit report. The credit bureaus and phone numbers are: 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** or 1-877-382-4357.

Consumers should never provide their personal information in response to an unsolicited telephone call, fax, letter, e-mail or Internet advertisement, says the Federal Deposit Insurance Corp.

The bottom line: **Don't get hooked by fraudulent phishing attempts!**

Presented by the
American Bankers Association