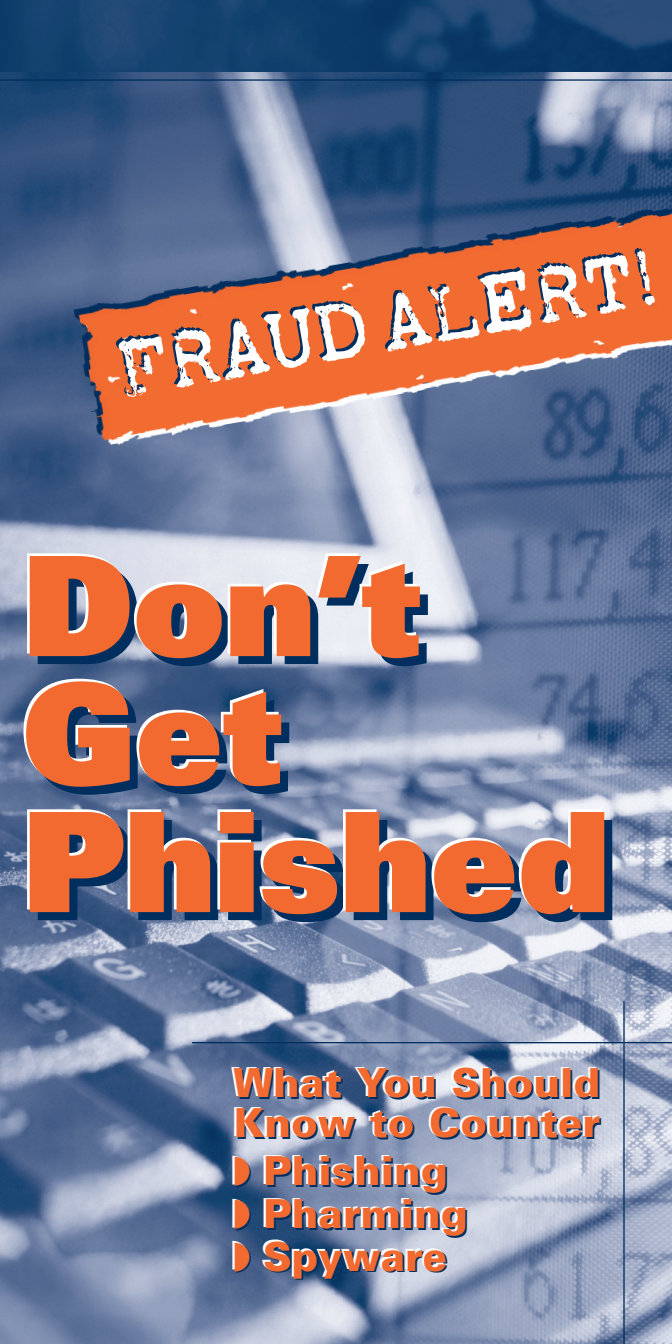
FRAUD ALERT!
Don't Get Phished
What You Should Know to Counter
Phishing
Pharming
Spyware

Protecting Yourself Against E-Mail Fraud

E-Mail and Internet Fraud take advantage of the Internet's unique ability to send e-mail messages worldwide in seconds or post Web site information that is accessible from anywhere. E-mail and internet fraudsters carry out their scams more invisibly than ever before, making identity theft from online scams one of the fastest growing crimes today.

You should be especially vigilant to these:

PHISHING Fraudulent e-mails, appearing to be from a trusted source such as your bank or a government agency, direct you to a Web site asking you to "verify" personal information. Once scammers have your information, they have the tools to commit account fraud *using your name*.

✔ What You Can Do:

- If you receive an e-mail that tells you to confirm certain information, **do not** click on the e-mail link. Instead, use a phone number or Web site address you know to be legitimate.
- Before submitting any financial information through a Web site, look for the "lock" icon on the browser status bar, or look for "https" in the Web address.
- Report suspicious activity (see resources section of this brochure).

Remember: Your bank will never send you an e-mail asking you to verify personal information!

PHARMING Similar to phishing, pharming seeks to obtain personal information by secretly directing you to a copycat Web site where your information is stolen, usually with a legitimate-looking form.

✔ **What You Can Do:**

- Be wary of unsolicited or unexpected e-mails from all sources.
- If an unsolicited e-mail arrives, treat it as you would a phishing source.

MALWARE Short for malicious software, and also known as "spyware," it is often included in spam e-mails. It then can take control of your computer and forward personal data to fraudsters.

✔ **What You Can Do:**

Install and update regularly your:

- Anti-virus software
- Anti-malware programs
- Operating system patches and updates

GENERAL TIPS AGAINST INTERNET FRAUD

- **Don't Judge by Appearances.** The availability of software that allows anyone to set up a professional-looking Web site means that criminals can make their Web sites look as impressive as those of legitimate businesses.
- **Be Careful Giving Personal Data Online.** If you receive e-mail requests for personal data, don't send the data without knowing who's asking.
- **Be Wary of Disguised E-mails.** If someone sends you an e-mail using an mail header that has no useful identifying data it could mean that the person is hiding something.

Here are some basic safety tips you can implement immediately:

- ***Password***—Experts advise a combination of letters and numbers.
- ***Virus Protection***—Your computer's anti-virus software needs to be up-to-date to guard against new strains.
- ***Spyware***—Anti-spyware programs are readily available. Every computer connected to the Internet should have the software installed…and updated regularly.

RESOURCES

- **Internet Fraud Complaint Center (IFCC): www.ifccfbi.gov**
- **Consumer Fraud (DOJ/Homepage): www.usdoj.gov**
- **Federal Trade Commission (FTC) Consumer Response Center: www.ftc.gov**
- **Consumer.gov: www.consumer.gov**
- **Identity Theft Resource Center www.idtheftcenter.org: 858-693-7935**