

# FRAUD ALERT

## *Don't Get Phished!!*

### Don't get hooked by Internet "Phishing" Scams

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.

- **STOP.** Resist the urge to immediately respond to a suspicious e-mail and to provide the information requested despite urgent or exaggerated claims. Know whom you are dealing with.
- **LOOK.** Read the text of the e-mail several times and ask yourself why the information requested would really be needed.
- **CALL.** Report anything suspicious to the proper authorities. Telephone the organization identified, using a number that you know to be legitimate. You can also contact the Internet Crime Complaint Center at [www.ifccfbi.gov](http://www.ifccfbi.gov) if you think you have received a phishing e-mail or have been directed to a "phishy-looking Web site.

### *If you've been "Phished"*

*If you believe that you have provided sensitive financial information about yourself through a phishing scam, you should take the following fraud alert measures.*

- **CONTACT.** Immediately notify your financial institution with the details of the event.
- **CONTACT.** Notify the three major credit bureaus and request that a fraud alert be placed on your credit report.
  - Equifax: 1-800-525-6285 P.O. Box 981222 El Paso Texas 79998
  - Experian: 1-888-397-3742 P.O. Box 9701 Allen, TX 75013
  - TransUnion: 1-800-680-7289 P.O. Box 2000 Chester, PA 19022
- **COMPLAIN.** File a complaint with the Federal Trade Commission at [www.ftc.gov](http://www.ftc.gov) or 1-877-382-4357.