

## OTHER SCAMS

- “Lotteries” or “sweepstakes” advise you that you have won money but they require money from you up front to buy something or to somehow ensure your chances of receiving your winnings.
- Buyers of something you have advertised for sale that insist on mailing payment by cashier’s check. Many times the check is for an amount larger than the purchased price and the buyer requests that the overage be sent back to him via money order. The cashier’s check is counterfeit.
- “Sponsors” or “charities” will push for contributions but will be reluctant to provide identifying information about themselves when questioned.
- The Nigerian and other similar scam letters, e-mails or faxes are from someone purporting to have money in his country that cannot be accessed because of “rules and regulations”. You are to be rewarded handsomely for your help getting this money back. All you have to do is provide your bank account information and money up front to take care of “necessary expenses”. You are, of course, asked to keep this plot a secret. Once they have drained all the money they can from you, you never hear from them again.

## PROTECT YOUR PERSONAL INFORMATION

Criminals want your personal account information and social security number. They can make huge profits at your expense. Don’t give them your information. Be suspicious of any electronic messages, phone calls or mail requests that ask for personal data. Find out more about phishing and other crimes at:

[www.antiphishing.org](http://www.antiphishing.org)

[www.ftc.gov](http://www.ftc.gov)

[www.usdoj.gov/criminal/fraud](http://www.usdoj.gov/criminal/fraud)

[www.idtheftcenter.org](http://www.idtheftcenter.org)

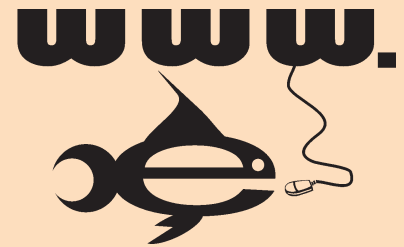


[www.banksecurity.com](http://www.banksecurity.com)



# PHISHING: Avoid Becoming a Victim

## FACTS YOU SHOULD KNOW®



Criminals are constantly improving their methods of stealing your personal financial information through fraudulent e-mails and Web sites designed to appear as though they were generated from legitimate businesses, financial institutions and even government agencies. This criminal activity is known as “phishing”. They are literally fishing for your personal information. This information is money in their pocket.

Grammatical errors and poor Web site quality used to be common identifiers of these phishing Web sites. Errors are not as common as before. Criminals improve their techniques with time, and this is evident in newer phishing messages.

This brochure will educate you on these scams, provide suggestions on how to avoid becoming a victim, and provide information on steps to take should you become a victim of phishing.

## AVOIDING THE SCAMS

- NEVER provide any personal information to an inquiry that is originated by someone else. Do not respond to e-mail inquiries even if they appear to be from a legitimate source. No financial institution, business or government agency will request you to confirm personal information. They already have that information if you have conducted busi-

ness with them before. Do not provide social security numbers, account numbers, credit card numbers, passwords, user name, etc.

- Always use a secure Web site when submitting credit card or other personal information in transactions that you initiate.
- Monitor your bank, credit card and other accounts regularly to ensure that all transactions are legitimate.
- Be suspicious of any e-mail notifications requiring you to act immediately to prevent an account from being closed or voided. Don't be intimidated!
- Protect your social security number.
- Don't use links that are provided in any suspicious e-mails.
- Apply security patches and be sure your browser is up to date. Two sites that provide support related to phishing scams are: <http://www.earthlink.net/earthlinktoolbar> and <http://www.microsoft.com/security/>.
- Contact your bank or other business if you become suspicious of any e-mail alleging to come from them.
- Report suspicious e-mail or phone activity to [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft) or via phone at 1-877-IDTHEFT.
- Sign up for the National Do Not Call Registry via FTC internet site or at 888-382-1222 (Federal Trade Commission). Your state may have its own Do Not Call Registry.
- Monitor your credit report at least annually.

## ADVICE FOR VICTIMS OF PHISHING

- Contact your financial institution(s) immediately.
- Contact one of the three major credit bureaus and request that a fraud alert be placed on your credit reports. Request a free copy of your credit reports. The law allows this free report once a year. The credit bureaus and contact numbers are:
  1. Equifax, 1-800-525-6285
  2. Experian, 1-888-397-3742
  3. TransUnion, 1-800-680-7289
- Visit [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft) to file a complaint with the FTC and to access a very useable Identity Theft Affidavit form you can use to alert lenders of your situation.
- Review all billing and bank statements immediately for accuracy.
- Close any affected accounts and open new ones.
- Contact local law enforcement and file a police report.
- Contact the Social Security Administration ([www.ssa.gov](http://www.ssa.gov)) if your SS number has been compromised.
- Document your activity.