Identity Theft Information

How To Protect Yourself

The best way to protect yourself from Internet fraud is to learn how to avoid becoming a victim. Unfortunately, Internet fraud is on the rise and anyone can be scammed and victimized. These scams can result in identity theft and financial loss. However if you become a victim, there is help available.

What is a Phishing Scam?

Typically, you'll receive an e-mail that appears to come from a reputable company that you recognize and do business with, such as your financial institution. In some cases, the e-mail may appear to come from a government agency, including one of the federal financial institution regulatory agencies.

The e-mail will probably warn you of a serious problem that requires your immediate attention. It may use phrases, such as "Immediate attention required," or "Please contact us immediately about your account." The e-mail will then encourage you to click on a button to go to the institution's Web site.

In a phishing scam, you could be directed to a phony Web site that may look exactly like the real thing. Sometimes, in fact, it may be the company's actual Web site. In those cases, a pop-up window will quickly appear for the purpose of harvesting your financial information.

In either case, you may be asked to update your account information or to provide information for verification purposes; your Social Security number, your account number, your password, or the information you use to verify your identity when speaking to a real financial institution, such as your mother's maiden name or your place of birth.

What is spyware and adware software?

The terms "spyware" and "adware" are essentially the same type of software. They are software that you may not be aware of running on your computer.

Spyware and adware is software that is installed on your computer, generally without your knowledge, that monitors or controls your computer's use. The software may send pop-up ads, redirect you to an un-requested website while you are on the Internet, monitor your Internet activity or record your keystrokes while you are online. This recording of keystrokes may lead to identity theft, on-line fraud or credit card fraud.

This same software may cause changes in systems, such as a mysterious change in opening Internet page, a new default search engine, an avalanche of pop-up ads while online, computer slow-downs or a computer crash. The biggest method of distributing spyware is to secretly bundle it with free software that you download from the Internet.

Keep your computer up to date with the latest security patches. Microsoft offers free updates at http://windowsupdate.microsoft.com and free CDs can be ordered for users on slow-speed dial-up. Install a personal firewall. Symantec and McAfee sell popular personal firewall, anti-virus, and anti-spyware software.

If you suspect your systems may be infected, please contact your computer consultant immediately.

Finally, practice safe surfing. That means downloading only trustworthy software, reading licensing agreements, avoiding banner ads, and deleting all spam without opening.

Identity Theft

The number of Americans who have experienced identity theft has surpassed 27 million, with the incidence rate increasing every year. At First Bank & Trust Co. we have substantial measures in place to protect your identity and your accounts against theft and fraud. For example, we have stringent bank privacy policies to protect your personal and financial information. Password protection for your online transactions help assure online security. When using our online services, you develop a secret password that only you know. Encryption of online transactions converts your information into secure code, protecting you against hackers.

Maximum security is possible ***only with your help!***

Here are some tips for protecting yourself:

- Never provide personal financial information, including Social Security number, account numbers or passwords, over the phone or the Internet if you did not initiate the contact.
- Report lost or stolen checks immediately.
- Never click on the link provided in an e-mail you believe is fraudulent. It may contain a virus that can contaminate your computer.
- Do not be intimidated by an e-mail or caller who suggest dire consequences if you do not immediately provide or verify your financial information.
- Closely guard your ATM Personal ID number and ATM receipts.
- If you believe the contact is legitimate, go to the company's Web site by typing in the site address directly or using a page you have previously book marked, instead of a link provided in the e-mail.
- If you fall victim to an attack, act immediately to protect yourself. Alert your financial institution. Place fraud alerts on your credit files. Monitor your credit files and account statements closely.
- Do not download or install any software unless you know and trust the source 100%.
- Clear out cookies and other tracking data on your computer regularly.
- Install software to counter-attack Spyware, Adware, Spam and pop-up ads.
- Download security patches and updates. Turn on automatic updates so you've got the latest fixes to problems as they arise.

Report suspicious e-mails or calls to the Federal Trade Commission through the Internet by clicking here, or by calling **1-877-IDTHEFT.** If you suspect that you are a victim of an Internet crime, visit the Internet Crime Complaint Center, www.ic3.gov and your local law enforcement.

Periodically contact the major credit reporting companies to review your file and make certain the information is correct.

Equifax (www.equifax.com)
800-525-6285
PO Box 740250
Atlanta, GA 30374

Experian
888-397-3742
Box 1017
Allen, TX 75013

TransUnion
800-680-7289
PO Box 6790
Fullerton, CA 92634