



left-hand) side of most Internet browsers. Most e-mail programs don't provide confidentiality via encryption, so be careful.

- Create "favorites" to access known sites and to avoid lures of imposter sites.
- Be sure to use updated anti-virus software. Some phishing e-mails contain viruses and software that can harm your computer. (See more on phishing below.)

### **Other Things You Can Do**

According to the Federal Trade Commission (FTC), the average identity theft victim doesn't learn he or she has been victimized until a year after the incident occurs. You may have been struck by an identity thief, if you:

- notice unexplained charges in, or withdrawals from, your accounts;
- receive credit cards for which you didn't apply;
- don't receive bills or other mail (which may indicate that an identity thief has changed your address);
- receive calls from debt collectors or companies from which you didn't order products.

***Check Your Credit Reports Annually.*** The Fair and Accurate Credit Transactions Act of 2003 allows you to get a free credit report from each of the three credit bureaus every 12 months. To better secure your financial credit, you should obtain and review a copy of your report at least once a year from:

- **Equifax**                **800 685-1111**
- **Experian**              **888 397-3742**
- **TransUnion**          **877 322-8228**

For more information, and to order your free credit report, visit the Federal Trade Commission at **ftc.gov**.

***Protect Your Social Security Number.*** Your Social Security number is a thief's primary tool for opening accounts in your name. You should, therefore, memorize your Social Security number; don't carry your Social Security card or leave it (or the number itself) in an easily accessible place. When making transactions, provide your Social Security number only if absolutely necessary. Find out if you can use other forms of identification, and ask why the company needs the number, how they will use it, and how they plan to safeguard it.

***Be Careful on the Phone.*** Identity thieves often pose as telemarketers, representatives of banks, Internet service providers or even members of government agencies — anything to get you to give out personal information like your Social Security number, date of birth or a mother's maiden name. So don't give personal information over the phone, through the mail, or on the Internet unless you've initiated the contact or are sure the company is legitimate.

If you have any doubts, contact the company's customer service department and ask how the information will be used, how it will be secured, and who will have access to it.

***Nail Down Your Mail.*** It's a federal crime to steal mail, but that doesn't deter identity thieves. Through stolen mail, thieves access credit card applications, bank account statements and other documents that contain vital personal information. Protect yourself by removing mail from your mailbox promptly. When traveling, contact your post office to receive a "vacation hold" card. When mailing letters or packages, go to the local post office or use post office collection boxes; avoid unsecured mailboxes.

***Keep a Lid on Your Trash.*** Some thieves stoop (literally) to picking through trash or recycling bins to unearth Social Security numbers, account numbers or other personal information. Keep your identity safe by using a crosscut shredder when destroying credit card receipts, financial statements, insurance forms, doctors' bills and other sensitive personal documents. When you use ATMs, never leave your receipts behind.

***Don't Get "Skimmed."*** Identity thieves sometimes obtain ATM pin numbers and other bank account information through a process called "skimming." Thieves "skim" by placing devices over ATM card readers, or even by inserting tiny cameras in or near the keypad. They capture your account information and use it to create fake ATM cards in your name, which gives them access to your accounts.

Avoid ATMs that have unusual features, such as devices attached to the card readers, or a sign telling you to swipe your card through a different reader than the one attached to the screen. Nonbank stand-alone ATMs — such as those in convenience stores — are especially susceptible to skimming.

***Keep Your Computer Safe.*** Thieves can hack into computers to access personal information. To safeguard your computer, update your virus protection software regularly. Also, install a firewall to prevent hackers from accessing your system. Don't download software from sites you aren't familiar with. If you make online financial transactions, be wary of "phishing," a scam through which thieves send e-mails or pop-up messages that request information like Social Security numbers and credit card account numbers. Generally, the wording in phishing communications is often careless and contains misspellings. If you receive an e-mail claiming to be from TIAA-CREF that seems fraudulent, please forward it to us immediately at [abuse@tiaa-cref.org](mailto:abuse@tiaa-cref.org).

Also be aware of "pharming," one of the newest scams, in which thieves hijack a domain a web address and then redirect it to a bogus site. If you receive any suspicious e-mail, delete it immediately. Don't attempt to respond to it or to click on any enclosed link.

For additional information on phishing and identity theft, visit the Federal Trade Commission at [ftc.gov](http://ftc.gov) and look for the following brochures: "How Not to Get Hooked by 'Phishing' Scam" and "ID Theft: When Bad Things Happen to Your Good Name."

***Lock Down Your Laptop.*** If you use a laptop, avoid storing important personal or financial information on it. Otherwise, use a "strong" password — a combination of upper- and lowercase letters, numbers and symbols.

***Be Suspicious of a Bullying or Frightening Tone.*** Demanding computer messages that threaten to terminate or suspend your account if you don't respond quickly are cause for concern. They

may say that if you fail to update, verify or confirm your personal or account information, access to your accounts will be suspended. Legitimate businesses don't request personal information from you over an unsecured website.

**Watch Out for Spoofing.** Web spoofing involves a fake website that mimics the legitimate site you were trying to visit. You might land there by accidentally keying in an incorrect web address, or by linking to it from a phishing e-mail.

To make spoof sites appear legitimate, identity thieves may use the logos, graphics, names and codes of the real company's site. They may also use a fake web addresses or bogus web tags, such as a ".org" or a ".edu," and the image of seemingly genuine "padlocks" on your web screen to entice you to believe it's safe to enter your personal information. If you take the bait, the spoof site may route your information — such as your Social Security number or other personal identification numbers, credit card information or financial account numbers — to identity thieves.

### **What to Do If You Become a Victim**

If you think you've become an identity theft victim, the FTC recommends following the steps:

**Contact the Social Security Administration.** Call the Fraud Hotline, **800 269-0271**.

**Contact the U.S. Department of Justice.** Visit the Justice Department's website at **[usdoj.gov/criminal/fraud/idtheft.html](https://www.usdoj.gov/criminal/fraud/idtheft.html)** for online guidance and a list of helpful articles.

**File a Complaint with the FTC.** The FTC provides assistance to victims of identity theft, as well as a free credit report. You can file your case with the FTC Consumer Response Center, at **[ftc.gov](https://www.ftc.gov)**.

To learn more, contact the FTC Identity Theft Clearing House hotline, **877 438-4338**. Another helpful FTC website is **[consumer.gov/idtheft](https://www.consumer.gov/idtheft)**, where you can access an online booklet, "*ID Theft: What It's All About.*"

**File a Police Report.** Send a copy of the report to creditors to show proof of the crime. Keep a copy of the report.

**Create A Fraud Alert Flag.** Contact the fraud departments of any of the three major credit bureaus to place a fraud alert on your credit file. This alert requests creditors to contact you before making changes to your existing accounts or opening new ones. You can also get a credit report from these agencies.

- **Equifax 800 685-1111** or **[equifax.com](https://www.equifax.com)**
- **Experian 888 397-3742** or **[experian.com](https://www.experian.com)**
- **Trans Union 877 322-8228** or **[transunion.com](https://www.transunion.com)**

**Close Affected Accounts.** If you know that accounts have been fraudulently opened in your name, close them immediately. If you open new accounts, use new pin numbers and passwords.

© 2008 Teachers Insurance and Annuity Association-College Retirement Equities Fund (TIAA-CREF), New York, N.Y. 10017

C42274