



What is Identity Theft?

Identity theft and identity fraud are terms used to refer to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain.

Preventive Measures You Can Take

1. Keep the credit cards you carry to a necessary minimum.
2. Maintain a list of phone numbers to all your credit card issuers for immediate use anywhere you travel.
3. Never carry your Social Security card. Do not give out your Social Security number unless you are legally required to do so. If requested to provide it, ask why it is necessary. If the answer is not convincing do not provide it.
4. Shred credit card offers you receive in the mail and all personal documents before you place them in the trash. Personal information in trash bags on your curb or in a land fill are not secure.
5. Obtain your credit report every year from the major credit bureaus and check for fraudulent activity. Make sure all entries are familiar to you.
6. Write to the three major credit bureaus to request that a fraud alert be placed in your record so a merchant will contact you if a request for a new credit account is received. There are three national credit reporting agencies: Equifax, Experian (formerly TRW) and Trans Union.
7. Take your name off promotional lists operated by credit reporting agencies and credit grantors. Contact the credit reporting agencies to request this.

What Should I Do If I've become A Victim of Identity Theft?

If you think you've become a victim of identity theft or fraud, act immediately to minimize the damage to your personal funds and financial accounts. Please take the following actions:

1. Contact the [Federal Trade Commission \(FTC\)](#) to report the situation, whether --
2. [Online](#),
3. By telephone toll-free at 1-877-ID THEFT (877-438-4338) or TDD at 202-326-2502, or
4. By mail to Consumer Response Center, FTC, 600 Pennsylvania Avenue, N.W., Washington, DC 20580.

Under the [Identity Theft and Assumption Deterrence Act](#), the [Federal Trade Commission](#) is responsible for receiving and processing complaints from people who believe they may be victims of identity theft, providing informational materials to those people, and referring those complaints to appropriate entities, including the major credit reporting agencies and law enforcement agencies. For further information, please check the [FTC's identity theft Web pages](#). You can also call your local office of the [FBI](#) or the [U.S. Secret Service](#) to report crimes relating to identity theft and fraud.

You may also need to contact other agencies for other types of identity theft:

1. Your local office of the [Postal Inspection Service](#) if you suspect that an identity thief has submitted a change-of-address form with the Post Office to redirect your mail, or has used the mail to commit frauds involving your identity;
2. The [Social Security Administration](#) if you suspect that your Social Security number is being fraudulently used (call 800-269-0271 to report the fraud);
3. The [Internal Revenue Service](#). If you suspect the improper use of identification information in connection with tax violations (call 1-800-829-0433 to report the violations).

Call the fraud units of the three principal credit reporting companies:

Equifax:

1. To report fraud, call (800) 525-6285 or write to P.O. Box 740250, Atlanta, GA 30374-0250.
2. To order a copy of your credit report (\$8 in most states), write to P.O. Box 740241, Atlanta, GA 30374-0241, or call (800) 685-1111.
3. To dispute information in your report, call the phone number provided on your credit report.
4. To opt out of pre-approved offers of credit, call (888) 567-8688 or write to Equifax Options, P.O. Box 740123, Atlanta GA 30374-0123.

Experian

1. To report fraud, call (888) EXPERIAN or (888) 397-3742, fax to (800) 301-7196, or write to P.O. Box 1017, Allen, TX 75013.
2. To order a copy of your credit report (\$8 in most states): P.O. Box 2104, Allen TX 75013, or call (888) EXPERIAN.
3. To dispute information in your report, call the phone number provided on your credit report.
4. To opt out of pre-approved offers of credit and marketing lists, call (800) 353-0809 or (888) 5OPTOUT or write to P.O. Box 919, Allen, TX 75013.

Trans Union

1. To report fraud, call (800) 680-7289 or write to P.O. Box 6790, Fullerton, CA 92634.
2. To order a copy of your credit report (\$8 in most states), write to P.O. Box 390, Springfield, PA 19064 or call: (800) 888-4213.
3. To dispute information in your report, call the phone number provided on your credit report.



4. To opt out of pre-approved offers of credit and marketing lists, call (800) 680-7293 or (888) 5OPTOUT or write to P.O. Box 97328, Jackson, MS 39238.

Contact all financial institutions where you have accounts that an identity thief has taken over or that have been created in your name but without your knowledge. You may need to cancel those accounts, place stop-payment orders on any outstanding checks that may not have cleared, and change your Automated Teller Machine (ATM) card, account, and Personal Identification Number (PIN).

Contact the major check verification companies (listed in the [CalPIRG-Privacy Rights Clearinghouse checklist](#)) if you have had checks stolen or bank accounts set up by an identity thief. In particular, if you know that a particular merchant has received a check stolen from you, contact the verification company that the merchant uses:

1. CheckRite -- (800) 766-2748
2. ChexSystems -- (800) 428-9623 (closed checking accounts)
3. CrossCheck -- (800) 552-1900
4. Equifax -- (800) 437-5120
5. National Processing Co. (NPC) -- (800) 526-5380
6. SCAN -- (800) 262-7771
7. TeleCheck -- (800) 710-9898

Phishing Scam Basics

What are Phishing and Pharming?

Phishing attacks use both social engineering and technical ploys to steal consumers' personal identity data and financial account credentials. Social-engineering schemes use 'spoofed' e-mails to lead consumers to counterfeit websites designed to trick recipients into divulging financial data such as credit card numbers, account usernames, passwords and social security numbers. Hijacking brand names of banks, e-retailers and credit card companies, phishers often convince recipients to respond. Technical schemes plant programs onto PCs to steal credentials directly, often using Trojan keylogger spyware. Pharming crimeware misdirects users to fraudulent sites or proxy servers, typically through DNS hijacking or poisoning.

5 Steps for Users to Protect Themselves from Phishing Scams

1. **Be Skeptical:** Unless you are 100% sure that a particular message is legitimate, assume it is not. You should never supply your username, password, account number or any other personal or confidential information via email and you should not reply directly to the email in question.
2. **Use The Old-Fashioned Way:** An even safer means of verifying if an email regarding your account is legitimate or not is to simply delete the email and pick up the phone. Rather than risking that you may somehow be emailing the attacker or mis-directed to the attacker's replica web site, just call customer service and explain what the email stated to verify if there is truly a problem with your account or if this is simply a phishing scam.
3. **Do Your Homework:** When your bank statements or account details arrive, whether in print or through electronic means analyze them closely. Make sure there are no transactions that you can't account for and that all of the decimals are in the right spots. If you find any problems contact the company or financial institution in question immediately to notify them.
4. **Make Sure Your Computer Is A Good HOST:** Your computer has a hidden system file called the Hosts file. This file can be used to hard code domain name translations and direct you to a different site. Normally if you try to visit paypal.com your computer sends the request to a DNS (Domain Name Server) which lets your computer know what the IP address of that domain name is so that your request can then be forwarded to the right server. The Hosts file supersedes DNS by adding an entry in the Hosts file with the domain name "paypal.com" and a different IP address so your computer is redirected to a different site. Rather than being sent to the true paypal.com server your request will go to the address specified in the Host file. You should periodically check your Host file to ensure there are no such malicious entries in there.
5. **Report Suspicious Activity:** If you receive emails that are part of a phishing scam or even seem suspicious you should report them. Douglas Schweitzer says "Report suspicious e-mails to your ISP and be sure to also report them to the Federal Trade Commission (FTC) at www.ftc.gov."