



What You Need to Know to Avoid Identity Theft





Table of Contents

Introduction	3
What is Identity Theft?	4
Important Identity Theft Facts	6
Types of Identity Theft	7
Financial Identity Theft	8
Criminal/Impersonation Identity Theft	9
Child Identity Theft	10
How Thieves Steal Your Identity	11
Online	12
Offline	14
Other Methods	15
How Identity Theft Affects You	16
How You Can Protect Yourself	19
General Tips	20
Online	21
Offline	22
What to Do if You Become a Victim	23
Resources: Additional Information	24
About McAfee	25

Introduction

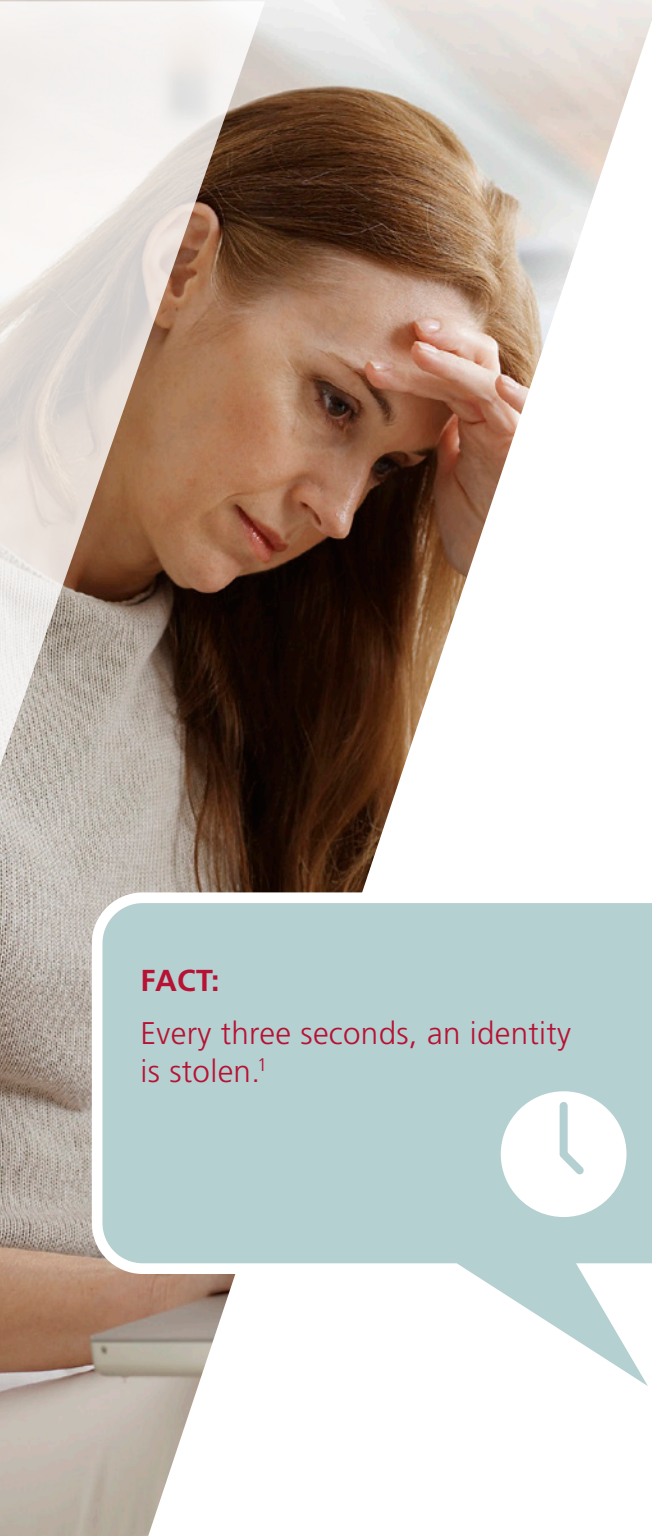
When you think of theft, you usually think of someone stealing your possessions. To avoid theft, you may have taken the trouble to install an alarm system in your home or lock up your valuables in a safe or a safety deposit box at the bank. But nowadays, possessions aren't the only things you need to protect. Modern thieves have gone high-tech—they can take your money, use your credit, and ruin your reputation by stealing your identity. Identity theft can happen to anyone because all of our personal information is scattered in so many places—from online shopping websites and corporate databases to wallets and scraps of paper. In this guide, you will learn more about how identity theft occurs and the measures you can take to protect yourself.





What is Identity Theft?

Identity theft, or identity fraud, occurs when someone steals information that defines your personal identity—such as your name, driver’s license number, passport number, bank account numbers, and credit card numbers—to reap the benefits of posing as you. These benefits can be financial, such as access to your accounts and credit cards, or they can be reputational in that thieves can use your identity to get a job or commit a crime.



Using your personal details, a thief can open a credit card account and run up charges, create counterfeit checks using your account number, or even obtain an official document, such as a driver's license or passport, in your name.

When this happens, you not only lose money, you also face losing the ability to take out a loan, or get a job due to bad credit and a damaged reputation. In severe cases, you could even be placed in jail for mistaken identity.

Most often, it takes a long time for victims to realise that their identities have been stolen, and by the time they become aware of the fraud the thief is long gone. This explains why it's so easy for thieves to commit identity theft and why it's so hard for law enforcement to catch them.

FACT:

Every three seconds, an identity is stolen.¹



¹ Identity Theft Protection site, <http://identityprotectiononline.com/2009/07/10/identity-theft-statistics/>



Important Identity Theft Facts

- The Home Office of the United Kingdom calculated the cost of identity theft to the British economy at £2.1 billion during the last three years²
- In the UK the most common form of identity theft information gathering occurs through the use of spyware³
- Credit card fraud losses in 2009 in the United Kingdom totaled £440.3 million⁴
- There were more than 51,000 phishing incidents recorded during 2009—a 16% increase on the amount seen in 2008⁵
- From 2005 to 2009, there have been more than 500 million consumers whose personal and financial data had been exposed as a result of corporate data breaches—events the victim cannot control despite taking personal safety measures⁶
- Victims spend an average of 58 hours repairing the damage done to existing accounts and an average of 165 hours repairing damage done by the creation of new, fraudulent accounts⁷
- 43% of identity theft occurs from a stolen wallet, checkbook, credit card, billing statement, or other physical document⁸



² <http://www.identitytheftsecrets.com/identity-theft-around-the-world.html>

³ Ibid

⁴ UK Cards Association - http://www.theukcardsassociation.org.uk/media_centre/press_releases_new/-/page/922/

⁵ Ibid

⁶ IdentityTheftInfo.com

⁷ Identity Theft Research Center. *Identity Theft: The Aftermath 2008*

⁸ Ibid



Types of Identity Theft

When most people think of identity theft they think of stolen credit cards or banking information, but there are actually various kinds of identity theft that can affect other important areas of your life, such as your finances, your reputation, and your child's credit record.

Let's take a look at the different kinds of identity theft so you can gain a better understanding of what you need to do to protect you and your family.



Financial Identity Theft

Financial identity theft involves using stolen personal information to get access to your money or credit. This is the most common type of identity theft because it is lucrative and often hard to trace. Problems resulting from financial identity theft include:

- **Unauthorised credit card charges**—Thieves who steal your credit card or misdirect billing statements to get ahold of your information can essentially take over your credit card account to make fraudulent charges. Criminals can also gain access to your account by intercepting new credit cards sent through the post or by applying for a new card with your personal information. When the thief fails to pay the charges they run up on your card, this can affect your credit, especially if it takes a while to figure out that your information has been stolen.
- **Bad credit**—If a thief uses your personal information to obtain loans, goods, and services and doesn't pay the bills, this can damage your credit.



Criminal/Impersonation Identity Theft

Criminal identity theft, or criminal impersonation, is when a thief takes over your identity and assumes it as their own. The thief could give your driver's license, date of birth, or passport number to law enforcement officers during an investigation or upon arrest. Alternatively, the imposter could present a counterfeit license containing your data.

Dangers of criminal identity theft include:

- **Criminal records**—If an identity thief commits a crime and presents himself to authorities using your name, then you could wind up with a criminal record or warrants for your arrest. You could even end up spending time in jail.
- **Traffic violations or warrants in your name**—If a thief steals your driver's license and commits traffic violations, they could present your identification to law enforcement officials. When they fail to pay the tickets or go to traffic court, you could be left with hefty fees and even warrants for your arrest.





Child Identity Theft

There is a growing trend among identity thieves to steal the identities of children, even infants, since a child's records represent a clean slate for the criminal and it usually takes years before the theft is discovered. Often, the first time victims discovers that their identity was stolen is when they engage in their first financial transaction and try to establish credit by, for example, purchasing a cell phone or buying a car.

The dangers of child identity theft include:

- **Damaged credit**—If many years pass before the victim realizes that their identity has been stolen, a long history of poor credit that is difficult to unravel may be the result.
- **Income tax liability**—If the thief has been working using a child's stolen identity, the child could be held liable for income taxes.


FACT:

The Identity Theft Resource Center reports that more than half (54%) of these crimes were committed against children under six years old.⁹



⁹ Federal Trade Commission, *About Identity Theft* microsite





How Thieves Steal Your Identity

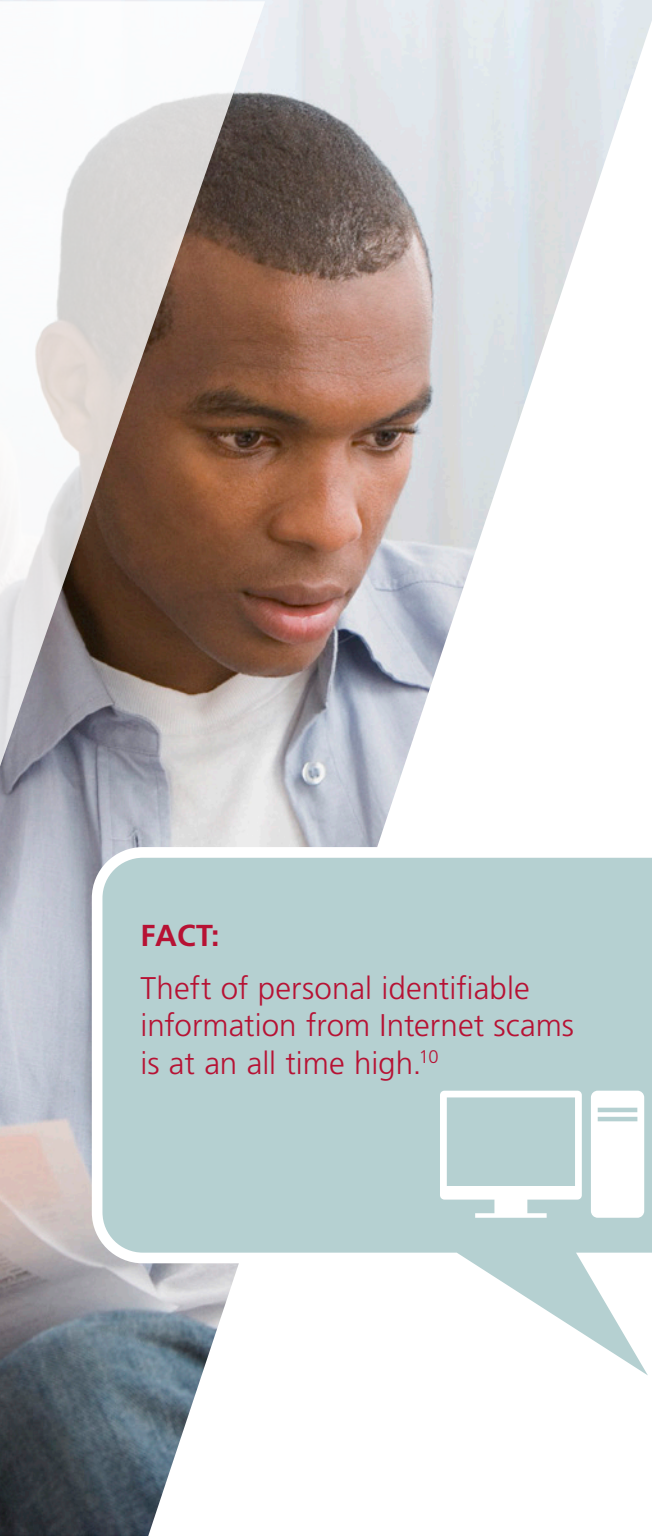
Identity theft is a growing problem. With that in mind, it's worth knowing how thieves can steal your identity. Unfortunately, they have numerous tricks up their sleeves—from old-fashioned methods such as stealing your wallet and raiding your mailbox to high-tech methods, such as data breaches and email scams.

Let's review some of the most common ways crooks can steal your sensitive information so that you can take preventative measures.

Online

- **Phishing**—Phishing scams are spam emails sent by cybercriminals that pretend to be from a legitimate person or organisation with the intent of tricking you into revealing personal information. For instance, a cybercriminal may send an email that looks like it originates from your bank asking you to “confirm” account information by clicking on a link that takes you to a fake website and asks you to type in your bank account user name and password. Phishing is one of the most common types of cybercrime, and thieves are constantly updating and changing their scams in hopes of fooling you.
- **Pharming**—In a pharming attempt, a hacker installs malicious code on your personal computer to direct you to fake websites without your knowledge. You could be directed to a fraudulent shopping site where you might enter your payment information without knowing that the site is not legitimate.
- **Spim**—Spim is spam sent via instant messaging (IM). The IMs could include spyware, keyloggers, viruses, and links to phishing sites.
- **Spyware**—This is software that a hacker surreptitiously installs on your computer to collect personal information. It can also be used to direct you to fake websites, change your settings, or take control of your computer in other ways.





FACT:

Theft of personal identifiable information from Internet scams is at an all time high.¹⁰



- **Keyloggers**—A keylogger is a form of spyware that records keystrokes as you type. The information you type is then saved to a file that the hacker can access. If you are surfing the web and visiting banking and e-commerce sites, a keylogger can potentially record your account and password information, which the hacker could then use to get access to your credit card or banking accounts and even steal your identity.
- **Trojan horse**—A Trojan horse is a malicious program that appears to be harmless. If you unwittingly download a Trojan horse from the web, it could allow the hacker remote access to your machine from anywhere in the world, which gives them the ability to access files on your computer and even watch your screen activity.
- **Social networking sites**—With so much popularity surrounding social networking sites, it's sometimes easy to forget that people outside your circle of friends can often access the information you post about yourself. By providing details such as your name, date of birth, contact details, and employer, thieves can start to piece together the information they need to steal your identity.
- **Wardriving**—Thieves also try to steal your personal information using a technique called wardriving, where they drive around looking for unsecured wireless connections (networks). If your home wireless connection is not secured, hackers can access data on all the computers you have connected to your wireless router, as well as see information you type into your banking and credit card sites.

¹⁰ Federal Trade Commission, *About Identity Theft* microsite



Offline

- **Mailbox raiding**—Thieves look to raid unlocked mailboxes. They are on the lookout for credit card, bank, and other financial statements which usually include account numbers. They also look for pre-approved credit card applications so they can open a new account in your name without your knowledge.
- **Dumpster diving**—In urban areas, crooks turn to a similar method: they dig through your rubbish looking for financial documents and papers that include sensitive information. Thieves can use the booty they find through mailbox raiding or dumpster diving to change your address and divert your billing statements in an effort to conceal the fact that your identity has been stolen.
- **Stealing wallets/checkbooks**—Wallet and checkbook theft may be the oldest trick in the book, but that's because it works. Many carry around not only their driver's license, but also their identification card, credit cards, and automated teller machine (ATM) cards, giving thieves all the information they need to impersonate their victims.
- **Stealing information from homes**—We tend to leave our bills and sensitive documents lying around the house and forget that family, visitors, at-home employees, and contractors can then easily access this information.
- **Address fraud**—A criminal can also easily change your address and redirect your mail to a different address so they can steal your confidential information or take over your banking or credit card accounts.
- **Shoulder surfing**—A criminal can get access to your pin number or password by simply watching over your shoulder as you are using an ATM or typing on your computer. Or they could be listening as you provide your credit card number or identification information over the phone to a legitimate vendor. Either way, they now have your data in hand and can commit serious crimes.

FACT:

In 42% of identity theft cases, victims reported that the imposter was a friend, family member, ex-spouse/partner, or someone in close contact with them such as a coworker.¹¹



¹¹ Federal Trade Commission, *About Identity Theft* microsite



Other Methods

- **Vishing/smishing**—Vishing and smishing are the same as phishing, except that vishing is done by telephone, and smishing is done by text message, although both often include an email component.

In a vishing attempt, a scammer may call you pretending to be from your bank to inform you that they have noticed some suspicious activity on your account. They would then ask you to “verify” account details over the phone.

In a smishing attempt, a scammer may send a link to a malicious website or a phone number that has an automated voice response system (a type of vishing) that asks for your personal information.

- **Skimming**—When you insert your ATM card into a compromised machine or run your credit card through a phony card reader, you could become a victim of skimming. Skimming is where a hacker illegally obtains information from the magnetic strip on the back of your credit or ATM card. This information can then be used to access your accounts or produce a fake credit card with your name and details on it.
- **Corporate data breaches**—Corporations of all sizes, whether they are healthcare providers, insurance companies, or online businesses, store a large amount of sensitive customer information. If this information is hacked or leaked, your personal and financial details may be exposed.

FACT:

ATM skimming costs consumers and companies more than \$8.5 billion a year.¹²



¹² <http://www.spamlaws.com/identity-theft-skimming>





How Identity Theft Affects You

Unlike the theft of a watch or stereo, identity theft can result in serious consequences that take both time and money to resolve, not to mention the emotional distress you may feel. Here are ways in which identity theft can affect your life and your future.

Financial Loss

Of course, the most obvious loss is financial. If the thief has access to your checking, savings, or investment accounts, they can steal funds from your account.

Damaged Credit

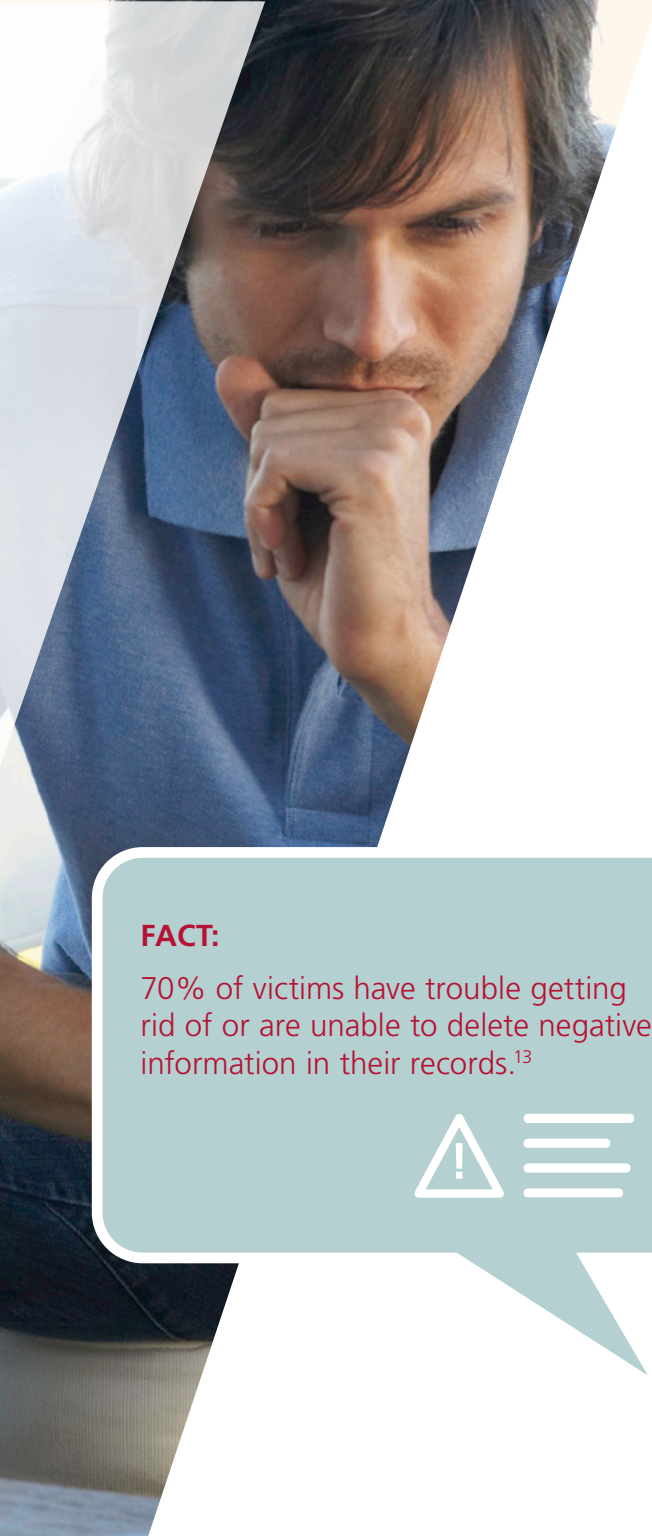
Because identity thieves open fake accounts at billing addresses that are different from yours, it's easy for them to run up charges without your knowledge. If these charges go unpaid, the delinquent accounts can show up on your credit report. You may not even realise that your credit has been damaged until you try to take out a car loan or mortgage and are denied credit.

Credit damage is particularly dangerous when it happens to children with stolen identities because it could be years before they attempt their first financial transaction and realise that their credit has been ruined.

Loss of Benefits

Identity thieves are often interested in other information beyond bank account numbers, such as your date of birth, address and passport number. Once they get ahold of these details, they can potentially obtain a driver's license in your name, receive benefits, and even land a job impersonating you.





Criminal Record

It may seem farfetched, but if a thief steals your identity and uses it to commit a crime, you could get a criminal record. A crook could obtain an identification card with your information and when that crook is arrested for a crime, the charges go on your record. And if the crook skips bail or doesn't appear before court, it's no loss to him because the authorities have a warrant out for you. The worse part is that you may not even know that you have a criminal record until you are pulled over for a traffic violation and arrested or when you apply for a job and are turned down after a background check.

The Cost to Repair Damage

Because it often takes a long time to realise that you've become a victim of identity theft, the damage can mount. Before you know it, you might be facing multiple fraudulent charges, damage to your credit report, and other issues that take considerable work and expense to repair. You can end up spending hours on the phone dealing with corporate and government bureaucracies trying to clear your name, and you may even decide to hire a credit repair service to help you. Even then, it may be years before you actually are able to clear the damage done to your reputation.

FACT:

70% of victims have trouble getting rid of or are unable to delete negative information in their records.¹³



¹³ <http://www.spamlaws.com/id-theft-statistics.html>





How You Can Protect Yourself

General Tips

- **Awareness and education**—Knowledge of the tricks and scams that thieves use to try to obtain your personal information can go a long way toward preventing identity theft. Be vigilant about sharing your personal details, and try to stay up to date on the latest scams.
- **Common sense**—Keep personal data private. When a person, website, or email asks for your personal information, ask yourself if it is standard practice for such information to be requested. Common sense will tell you that your bank would never send you an email asking you to confirm your account number, user name and password or ask for details like your passport or driver's license number.
- **Be aware of those around you**—Be mindful of your environment and others who may be in proximity when you make purchases over the phone, type in your ATM PIN, enter your credit card while shopping online, or text personal information. And remember to never send your credit card or account numbers to anyone via email.



Online

- **Online protection**—When you are surfing the web, use a comprehensive security suite, such as McAfee® Total Protection™ software, which not only protects you against viruses, spyware, and other emerging threats, but also provides safe search technology to help you steer clear of fake websites that try to collect your information.

In addition, make sure you use a firewall to block unauthorised access to your computer or network.

- **Use strong passwords**—Passwords should be at least 10 characters long and should consist of a combination of letters, numbers, and special characters. Also, consider changing your passwords periodically to reduce the likelihood that thieves can appropriate them and misuse them. Do not share passwords with anyone—not even with friends and family.
- **Practice safe surfing on public hotspots**—If you are using a public computer or accessing the Internet from a public hotspot or an unsecured wireless connection, do not log in to banking and credit card sites. Do your surfing at home on a secure network.
- **Secure your wireless network**—To prevent wardriving, enable the firewall on your router and change the administrator's password. Most routers come with a default user name and password, allowing you to set up and configure the router, but hackers are often familiar with these defaults. You may also want to change the default identifier on your router that is used to announce its presence to devices in the immediate area and permit access only from computers or devices you designate. Check your router's user manual to find out how to change these default settings.



Offline

- **Review your financial statements promptly**—Check your credit card and bank statements each month to make sure there are no fraudulent charges and to confirm that you authorised all transactions.
- **Shred documents**—The only way to keep thieves from digging up your personal information from the rubbish is to shred sensitive documents, such as financial statements, credit card offers, and expired driver's licenses.
- **Get a locked mailbox**—If you live in a residence with communal area for post get a mailbox that only you can access.
- **Keep your documents safe**—Put personal documents in a lockable drawer, safe, or cabinet at home, and consider storing valuable financial documents such as stock certificates at your bank.
- **Monitor credit history**—Because it can take a long time to discover that you've become a victim of identity theft, you should monitor your credit history to see if there are accounts or delinquent payments of which you may be unaware. There are a number of websites that offer free access to your credit reports, as well as paid services that monitor your credit for you.
- **Use a protection service**—Identity protection services help safeguard your identity by monitoring your credit, as well as providing proactive protection, such as sending notifications when new accounts are opened in your name. These services are usually provided for a monthly fee that includes free access to your credit reports.



What to Do if You Become a Victim

If you discover that your identity has been compromised or stolen, take immediate steps to address the situation.

1. Notify the credit bureaus and create a fraud alert

Call the fraud department of the credit bureaus and notify them of the situation. They can set up fraud alerts on your account that will require creditors to call you before extending credit.

2. File a police report

If you know your identity has been stolen, file an identity theft report with your local police department, which maintains a list of fraudulent accounts. Keep a copy of the report so you can give the number of your investigator to creditors and others who may ask you to verify that your identity has been stolen.

3. Contact financial institutions and agencies where your accounts may be affected

Call your bank and creditors to inform them of the situation and flag any fraudulent charges or withdrawals from your accounts and then follow up in writing. Verify that the charges have been removed from your accounts, and if necessary close the account. Keep copies, document conversations, and maintain records related to the theft.

4. Put a credit freeze in place

You can block thieves from opening new accounts in your name by freezing or locking access to your credit file at the three credit bureaus. If a thief tries to open a new account, he will be denied credit because the potential creditor or service provider will not be able to check your credit file.

5. Consider legal help or an identity restoration specialist

If you feel overwhelmed by the extent of the damage, you may want to consider hiring legal counsel to help you deal with debt collectors, credit bureaus, and creditors. Identity restoration specialists can also help guide you through fixing the problem. For instance, you can call the McAfee Cybercrime Response Unit for free advice on what to do in the case of identity theft.

Resources: Additional Information

Below are some sites that can help you understand more about identity theft and fraud and how to protect yourself.

Identity Theft Information

Identity Theft Resource Center

<http://www.idtheftcenter.org/>

Identity Theft Assistance Center

<http://www.identitytheftassistance.org/pageview.php?cateid=19>

Home Office Identity Fraud Steering Committee

<http://www.identitytheft.org.uk>

About Identity Theft

<http://www.aboutidentitytheft.co.uk/>

McAfee Cybercrime Response Unit

<http://www.mcafee.com/cru>

CardWatch

<http://www.cardwatch.org.uk/>

Report Phishing

Anti-Phishing Working Group

reportphishing@antiphishing.org

Bank Safe Online

reports@banksafeonline.org.uk

Fraudwatch International

scams@fraudwatchinternational.com

Government Agencies

National Fraud Reporting Centre

<http://www.actionfraud.org.uk/>

To report fraud: 0300 123 2040

CIFAS

<http://www.cifas.org.uk>

Royal Mail

<http://www.royalmail.com>

Customer Enquiry Number: 08457 740740

Identity & Passport Service (IPS)

To report lost or stolen passport:

<http://www.direct.gov.uk/en/TravelAndTransport/Passports/Loststolenordamagedpassports/index.htm>

National Fraud Authority

<http://www.attorneygeneral.gov.uk/nfa/Pages/default.aspx>



