How To Keep Your Privacy And Identity Protected From Everything

Table of contents

What about your right to privacy? 4
Privacy protection – what are they looking at and how to stop them? 12
Are you the master of your identity? 17
Identity Thieves – What's the real threat? 18
What You Can Do to Prevent Identity Theft 20
Credit Cards - Becoming less vulnerable 28
Online Shopping Credit Card Protection 30
Protect Yourself from Identity Theft at the ATM 31
Mailboxes and Identity Theft 32
Job Scams 34
Danger Where You Never Would Expect It 35
More Tips for Making Yourself Safer from Identity Theft 36
Protecting yourself online 40
What If You Become A Victim of Identity Theft 42
Stop Identity Theft at work 49
Tips for Protecting Your Social Security Number 50
What to do if you are the victim of a criminal identity theft? 52
Tax Filing Tips 53
Steps to Take If You Are a Victim of Tax Identity Theft 55
Identity Theft Insurance 56
Factors to Consider When Buying Identity Theft Insurance 57
Protecting Your Privacy—A Key to Preventing Identity Theft 60
Privacy Settings on Facebook 60

Protecting Your Privacy on Google 64

Dangers of Data Gatherers 64

Steps to Take to Increase Your Privacy 66

Identity Theft and the Elderly 68

Medicare Identity Theft Threats 70

How to Help Prevent Elderly Identity Theft 72

Signs of Elderly Identity Theft 75

Recap - Identity Theft Protection Rules 75

Recap - Rules to Follow If You Are a Victim of Identity Theft 82

What about your right to privacy?

With the recent revelations that the NSA and other agencies have been tapping into corporate streams of data that can provide them with massive amounts of private information about U.S. citizens, now is a good time to start thinking about how best to keep your private information private.

According to the Department of Justice's most recent National Crime Victimization Survey, "In 2010, 7% of households in the United States, or about 8.6 million households, had at least one member age 12 or older who experienced one or more types of identity theft victimization." That's almost one in 10, with 76% of them experiencing direct financial loss as a result.

Citizens of the United States are afforded a number of rights. These rights have evolved and developed over the centuries and have been added to the permanent record in the form of amendments to the Constitution of the United States.

As it stands right now, there are a total of 27 amendments. A couple of them cancel each other out like the 21st amendment which repeals the 18th amendment prohibition on the manufacture, sale or transportation of alcoholic beverages.

Most United States citizens are probably not aware of what is written in those amendments. They may have memorized it long enough to pass a high school government or civics class, but that data has long since been purged to make room for more important things. Many Americans are probably unaware that it was not legal for the United States government to collect income taxes until they passed the 16th amendment or that a person could be President indefinitely until the two term limit was imposed by the 20th amendment.

Amendments such as the 1st amendment right that essentially defines the separation of church and state, the 2nd amendment right to bear arms, or the 4th amendment protecting you from unlawful search and seizure of your property are fairly common knowledge and are mentioned frequently in the media in support of various causes.

Alright, but anything about privacy? The 14th amendment is often cited as the amendment which protects what Justice Louis Brandeis called the “right to be left alone”, but upon reading it, it appears that a fair amount of interpretation has to be allowed for in order to come to the conclusion that it inherently protects our privacy. The 1st, 4th and 5th amendments are also occasionally referred to in discussions of a right of privacy.

Of course, the 10th amendment explicitly grants authority to the individual states for any power not delegated to the United States Congress or prohibited explicitly in the Constitution of the United States. So, there may very well be provisions protecting privacy in state constitutions or state laws. There are also a number of statutes and regulations at both the federal and state levels which are based at least in part on the inferred right of privacy.

Unfortunately, privacy, and the protection of sensitive or personal information, seems to be legislated on an industry by industry basis. The Privacy Act of 1974 prevents the unauthorized disclosure of personal information held by the federal government. The Fair Credit Reporting Act protects information gathered by credit reporting agencies. The Children's Online Privacy Protection Act grants parents authority over what information about their children (age 13 and under) can be collected by web sites.

As technology marches forth and new innovations come along that make life simpler, more efficient or more convenient, these benefits often come with a trade-off of some privacy.

If you call to order a pizza you are typically asked for your phone number. You could refuse to share that information if you feel that it is none of their business and you want to protect that personal information. But, by sharing your phone number with the pizza

place, they are able to access your address in the blink of an eye so they know where to deliver the pizza without you having to tell them each time. Some pizza places are even sophisticated enough to keep track of what you have ordered so you can just order "the usual" without having to specify the details of the order every time you call.

When you go to the Amazon.com web site, you are greeted with a home page that says "Hello, Your Name" with a tab at the top of the screen called "Your Name's Store" which displays items you have shown an interest in or related items that Amazon recommends you take a look at based on your past shopping habits and known preferences.

But, this convenience and technical efficiency means compromising your privacy at least a little. If you want to save the time and hassle ordering pizza, the pizza place has to store your name, phone number and home address, and possibly even your ordering history, in a database somewhere. To receive your personalized Amazon.com treatment and customized recommendations you have to allow Amazon.com to store some of your personal information including your shopping habits and items you have searched for in the past, as well as allowing them to place a cookie on your computer that identifies who you are to their servers.

In doing so, you trust that the companies you choose to do business with and share your personal information with will treat that information with the appropriate level of discretion and security. You trust that they won't turn around and sell your personal data to a junk-mail marketing firm or store it in a text file on an insecure computer that anyone can access from the Internet. If you don't have confidence in the intentions or abilities of the company you are working with, you should think twice about sharing your personal information.

Whether written explicitly in concrete terms or implied through statutes, regulations and precedent-setting case law, it appears that people are generally in agreement that there exists a right to privacy and that the government and law enforcement must act on our behalf to guarantee it. While most Americans may not be able to recite the amendments to the Constitution, and may not even know much about the Constitution itself, there is an underlying trust from most people that the government will operate within the bounds of the Constitution and that every effort will be made to protect the rights granted to us by the Constitution, even if we don't know what they are.

Unfortunately, security and privacy are often in conflict. To provide better security, law enforcement agencies could keep detailed

profiles of every citizen and constantly track and monitor your every move. By doing so, would-be thieves, terrorists and or other bad guys could be thwarted before they attack or at least be more easily apprehended. Of course, as citizens, we are not generally willing to sacrifice the security of all just so that the infinitesimally small percentage of the population that are bad guys can be caught.

Instead, our society has come up with various trade-offs that seem reasonable enough to allow for the privacy of the general population while also enabling law enforcement to track bad guys. The 4th amendment of the Constitution protects citizens from unlawful search and seizure of personal property, but it also grants law enforcement the ability to obtain a search warrant if there is enough evidence to suggest that there is probably cause to suspect someone of doing something wrong.

However, in the wake of the terrorist attacks on September 11, 2001, the USA-PATRIOT Act removes many of those safeguards in the interest of national security. Gripped by fear, people accepted the PATRIOT Act as “necessary” without stopping to think of the impact it could have on law-abiding citizens or whether or not the rights they were forfeiting would actually result in a more secure nation. Essentially, the government or law enforcement can simply dub an individual a “person of interest” and the rights afforded by

the Constitution are virtually null and void. Changes have been made to reduce the red tape necessary for law enforcement to wire tap or search a suspect and “persons of interest” may be detained indefinitely without being charged and without the benefit of legal counsel.

The government is in favor of protecting your privacy, but only as it relates to other companies or individuals acquiring it. For the most part, they would prefer to have your complete details recorded and reserve the ability to access any part of your life or personal data that suits them.

The NSA (National Security Agency) and the United States government got very testy and even threatened to charge Phil Zimmerman with treason when he created the PGP encryption algorithm and allowed it to be exported internationally via the Internet. They were primarily upset because they couldn’t break the encryption either and they did not want people to be able to encrypt things so well that the government themselves could not access it. There have been bills introduced repeatedly in the past decade trying to mandate some sort of secret back door that grants the government the omnipotent key to bypass any security measures in computer hardware or software.

One of this country's Founding Fathers and an all-around source of wisdom, Benjamin Franklin, is credited with having said "They who would give up an essential liberty for temporary security, deserve neither liberty or security".

The problem is that, once a line is drawn, it is never completely erased. The line may be moved left or right depending on societal pressures or who the dominant party in power is, but the danger is in allowing a line to be drawn in the first place. The United States income tax, which began as a temporary means of raising money to support a war-effort, persists over a hundred years later and has morphed into its own bureaucratic juggernaut and spawned an entire industry of lawyers, books, software, and services.

The PATRIOT Act was created as a temporary measure, but almost as soon as it was passed the lobbying began for extending the expiration dates of some of the provisions or just implementing the legislation on an indefinite basis. Now that the power has been granted, it is very difficult to take back. Ostensibly, if you are an upstanding, moral citizen, the removal of basic rights granted by the PATRIOT Act should not affect you. But, who is to say who decides what makes you moral or upstanding? You may be on the right side of the line now, but what happens when the line gets moved and you suddenly find yourself a "person of interest"?

Ultimately, it is up to you to choose a balance that works for you. How much privacy are you willing to trade in order for more convenience and efficiency as a consumer? How much privacy are you willing to surrender with the hope that it will help the government secure and protect the nation?

Privacy protection – what are they looking at and how to stop them?

1. Your phone

If you're looking to keep SMS messages secure and you have an iPhone, there's a free app called Wickr that can help. The app uses end-to-end encryption without storing the keys for decryption on its servers. What that means is that when you send a message to someone else using Wickr, nothing you say can be read by anyone at Wickr. Because of that, there's no stream of plain text messages going back and forth that the NSA or anyone else can siphon.

If you're an Android user, you have a few more options than iPhone users do. For text messages, there's Gibberbot. Like Wickr, Gibberbot is free and promises more secure messaging.

And for calls, check out RedPhone. When calling someone who also has RedPhone, everything you say is encrypted, making it much more difficult for someone to listen in. Plus, it's free and uses your

data connection, not your cellular voice. So not only will your calls be secure, you won't have to pay for the minutes either.

2. Your Dropbox

According to documents released by The Guardian and The Washington Post, Dropbox is "coming soon" to the NSA's spy program. If that were to happen, documents, tax records or other private information in your Dropbox folder could be subject to government monitoring. Add to that Dropbox suffering security breaches in the past, and they're just not safe enough for me. The solution? SpiderOak.

SpiderOak is just like Dropbox -- there's a folder, you put stuff in it, that folder syncs between computers and devices -- but with one important difference: good encryption. Everything you put in your SpiderOak Hive (that's what they call their syncing folder) is first encrypted on your computer using your password, then sent to the SpiderOak servers.

This means that even SpiderOak can't read your data without your password; it looks like gibberish. So if someone (the NSA, a foreign government, or a hacker in Latvia) manages to get into SpiderOak's servers, they won't be able to see what you've stored there without

breaking one of the world's most advanced encryption algorithms (one the NSA trusts to secure its own data).

But SpiderOak can also back up any file or folder on your computer, sync any file or folder on your computer, and share any file or folder on your computer. This makes it a great one-stop-shop for all your syncing, sharing and backup needs.

There's a free plan that offers 2 GB of data, plenty for storing tax returns, scans of important documents, photos, small videos, and other data that you would prefer was stored securely. If you need more space, they offer it for a fee. Prices are almost identical to Dropbox, starting at $10 for 100 GB.

3. Your credit cards

Yes, the NSA is probably looking at credit card transactions, too. So how do you get around exposing your purchase history? "I already know this; the answer is to use cash," you're probably thinking. But how do you shop online without using a credit card?

The answer is Bitcoin. It's a virtual currency (you give or receive Bitcoins, which are worth something in dollars), but if used correctly, it can provide almost complete anonymity when shopping online. And since you're not typing your credit card information into

a site that may or may not keep that data secure, there's no risk that your account will be stolen by someone hacking the site.
The only catch is that there aren't a lot of places that accept Bitcoins. In fact, you'd be hard-pressed to find ones that do. But if the currency takes off, it could become the "cash" of the Internet.

A more doable option? Buy prepaid gift cards from Visa, MasterCard or American Express with cash. Then use those to shop online. You'll probably have to pay a few dollars extra when buying the card, but afterward you'll be able to shop anywhere those cards are accepted without having the purchase data and your identification forwarded to a government agency.

If the site where you used the card is ever hacked, you've got nothing to worry; by that time you'll probably have already used the balance on the card and moved on to one with a different number.

4. Your Web history

Everything you search for on Google, and a good deal of your browsing activity, can also be snooped on by the NSA, according to news reports. The problem is your IP address. It's the sequence of numbers that identifies your computer on the Internet, and can be traced back to you through your ISP (Internet service provider).

The answer? A virtual private network, or VPN. A VPN will sit between you and the websites you visit, encrypting and relaying information back and forth. So when you do a search on Google, the IP address Google records as having performed the search is that of the VPN, not you. Find a good VPN, one that's easy to use, with a good price, limited or no logging of your activity and fast speed, and you'll be much harder to track online. Just make sure you sign out of your Google, Facebook, and Twitter accounts before connecting to the VPN, or use your Web browser's private mode.

Here's a list of VPNs to consider. If you just want me to pick one for you, check out IPVanish.com. They have software that makes them especially easy to use, can be set up on your computer, tablet or smartphone, have servers all over the world that you can connect to, and cost $10 for unlimited use (and it's even cheaper if you pay for a year in advance).

Bonus: Some VPNs accept Bitcoin as payment, making for the ultimate in anonymous Web browsing. Not even the VPN has to know who you are.

While using a VPN at home is something you might consider to protect your privacy from the NSA, using a VPN at a public Wi-Fi hot spot or hotel network should be mandatory. Often, those networks are unsecured and almost everything you do can be "sniffed" out of

the air by someone else connected to the same network. A VPN would protect you.

5. General protection

While I've tried to hit all the major areas you might want to protect, this is by no means a comprehensive list of everything you can do to keep your private information safe and secure. Entire websites could be devoted to the topic.

Websites like Security In-A-Box. They'll teach you everything from creating good passwords and protecting your computer from hackers to remaining anonymous online and bypassing censorship. And it's free. If you're interested in protecting your data in this brave new world, I encourage you to check it out.

Are you the master of your identity?

Identity theft is one of the most pervasive and insidious crimes of today, a crime that can tremendously disrupt your life— or even put you in jail for crimes you never committed.

I will show you just how vulnerable you are, but you will also read steps you can take to protect yourself, as best you can, from becoming a victim and what to do if you become an identity theft victim. Identity theft is the biggest and fastest-growing crime in the

world, and with good reason. It is easy to perpetrate and easy to get away with. No one is immune from identity theft— children, the elderly, and even the dead can have their identities stolen.

In this age of information sharing, everyone is particularly vulnerable to identity theft because even if you are doing everything right, the many companies and institutions with which you do business and operate in your everyday life might not be protecting you as much as they can. I can show you how to minimize those risks.

Identity theft can result in your being hounded by debt collectors for debts you did not incur; becoming unable to access your own credit cards, bank accounts, or brokerage accounts; being arrested for crimes committed by people who have stolen your identity; or even receiving improper medical care because your medical identity has been stolen and your medical records have been corrupted. In addition, identity theft can ruin your credit rating, which can affect your chances to get a loan, get a job, get insurance, or rent a home.

The time, money, and effort that it takes to repair the harm done by identity thieves can be tremendous.

Identity Thieves – What's the real threat?

Identity thieves take your personal information and use it to harm you in a number of ways, including these:

• Gaining access to your credit card account, bank account, or brokerage account

• Opening new credit card accounts in your name

• Opening new bank accounts in your name

• Buying cars and taking out car loans in your name

• Buying cellphones in your name

• Using your name and credit to pay for utilities, such as fuel oil or cable television

• Using your medical insurance to obtain medical services, thereby corrupting your medical records

• Renting a home

• Using your name when committing crimes

Although you might not be responsible for fraudulent charges, the damage to your credit as reflected in your credit report can affect your future employment, insurance applications, and loan applications, as well as any future credit arrangements you might want to establish.

What You Can Do to Prevent Identity Theft

As damaging as identity theft can be and as vulnerable as we are to identity theft, there are a number of relatively simple things that you can do to make yourself less likely to become a victim of identity theft:

1. Do a little spring cleaning in your wallet or purse, even if it is the middle of the summer. Do you really need to carry all the cards and identifications that you presently carry?

2. If you rent a car while on vacation, remember to destroy your copy of the rental agreement after you have returned the car. Don't leave it in the glove compartment.

3. Stolen mail is a ripe source of identity theft. When you are traveling, you might want to have a neighbor you trust pick up your mail every day or have your mail held at the post office until your return. Extremely careful people or extremely paranoid people, depending on your characterization of the same people, might prefer to use a post office box rather than a mailbox at home. Identity thieves also get your mail by filling out a "change of address" form using your name to divert your mail to them. If you find you are not receiving any mail for a couple of days, it is worth contacting your local postmaster to make sure everything is okay. A

recent preventive measure instituted by the U.S. Postal Service requires post offices to send a “Move Validation Letter” to both the old and the new address whenever a change of address is filed.

If you receive one of these notices and you have not changed your address, you should respond immediately because it could well be a warning that an identity thief has targeted you. A careful credit card holder keeps an eye on his or her mailbox for the arrival each month of his or her monthly statement from the credit card company. If a bill is missing, it might mean that someone has hijacked your account and filed a change of address form with the credit card issuer to buy some more time. The sooner you become aware that the security of your account has been compromised, the better off you will be. You should also be particularly watchful of the mail when your card is close to expiration. An identity thief might be in a position to steal your mail containing your new card. If an identity thief is armed with enough personal information to activate the card, you could be in trouble.

4. Prudent people might want to use travelers’ checks while on vacation rather than taking their checkbook because an enterprising identity thief who manages to get your checkbook can access your checking account and drain it.

5. Be wary of who might be around you when you use an ATM (automated teller machine). Someone might be looking over your shoulder as you input your PIN (personal identification number). That same someone might lift your wallet shortly thereafter. Next step— disaster.

6. Make copies of all your credit cards, front and back, so that you can tell whether a card has been lost or stolen. Also keep a list of the customer service telephone numbers for each card. When copying your cards, you might want to consider whether you really need that many cards.

7. Be careful when storing personal information and mail, even in your own home. Shreveport, Louisiana, police arrested a baby sitter on identity theft charges. They alleged that she stole a credit application mailed to the people for whom she was baby-sitting and also opened other accounts using the Social Security number of her employer that she had found while rummaging through their documents.

8. After you have received a loan, a credit card, or anything else that required you to complete an application containing your Social Security number, request that your Social Security number be removed from the application kept on record. In addition, if you are feeling particularly paranoid, ask that your credit report used by the

bank or other institution be shredded in your presence. They no longer need that information after you have received the loan.

9. Make life easier for yourself. Remove yourself from the marketing lists for preapproved credit cards and other solicitations. You can remove yourself from the Direct Marketing Association's solicitation list by writing to them at Mail Preference Service, Direct Marketing Association, P.O. Box 9008, Farmingdale, NY 11735. Include your name and address, but no other personal information. You can also take yourself off of the list of preapproved credit card offers for five years by going online to www.optoutprescreen.com. Register for the Direct Marketing Association's Mail Preference Service to opt out of national mailing lists online at www.dmaconsumers.org, but there is a $ 5 charge for doing so if you do it online. You also can print out the form and get yourself removed from mailing lists at no cost. Additionally at the same Web site, you can also remove yourself from commercial email solicitations. When you go to www.dmaconsumers.org, go to the Consumer FAQs page, where you will find the links to remove yourself from these mailing lists. DMA members are required to remove people who have registered with the Mail Preference Service from their mailings. However, because the list is distributed only four times a year, it can take about three months from the time that your name has been entered to see a reduction in junk mail. It is also important to remember that many

spammers are not members of the Direct Marketing Association, so you can still expect to get some spam emails and snail mail.

10. If you do get unwanted spam e-mails, do not click on the "remove me" link provided by many spam e-mails. All you will succeed in doing is letting them know that you are an active address, and you will end up receiving even more unwanted e-mails.

11. If you receive spam faxes, you also should be wary of contacting the telephone number to remove yourself from their lists. It is already illegal for you to have received the spam fax. Contacting the sender by its telephone removal number might cost you for the call and will not reduce your spam faxes.

12. Sign up for the National Do Not Call Registry to reduce unwanted telemarketing calls. Most telemarketers are legitimate. Almost all are annoying, and many are criminals setting you up for identity theft. To sign up for the Do Not Call Registry, you may call toll free 888-382-1222 or register online at www.donotcall.gov.

13. Check your credit report at least annually and remember to get copies from each of the three major credit report bureaus, all of which independently compile the information contained in their files. Federal law permits you to annually obtain a free copy of your credit report from each of the three major credit-reporting agencies:

Equifax, TransUnion, and Experian. You can get your free credit reports by going to www.annualcreditreport.com or by calling 877-322-8228. It is important to note that there are a lot of companies that appear to be offering free credit reports, but if you read the fine print (and rarely will you find anything fine in fine print), you will see that often when you sign up for a "free" credit report, you have also signed up for a costly monthly service to follow. The only official Web site from which you can truly obtain your credit reports for free without any conditions is www.annualcreditreport.com. You also might want to consider staggering the obtaining of your credit reports by ordering one of your free credit reports from each of the three major credit-reporting agencies every four months so that the information you receive is more current. Look over your file and make sure everything is in order. Particularly look for unauthorized and inaccurate charges or accounts. Also, check out the section of your report that deals with inquiries. A large number of inquiries that you have not authorized could be the tracks of an identity thief trying to open accounts in your name. A large number of inquiries can also have the harmful effect of lowering your credit score.

14. Check your Social Security statement as provided by the Social Security Administration annually. It provides an estimate of your Social Security benefits and your contributions and can be helpful in detecting fraud. It is also a good thing to check this statement

carefully each year to make sure that the information contained within it is accurate to ensure that you are slated to receive all the Social Security benefits to which you are entitled.

15. Don't carry your Social Security card with you. You don't need it with you at all times, and if your wallet or purse is lost or stolen, you have handed over the key to identity theft to a criminal.

16. Carefully examine your monthly bank and credit card statements for any discrepancies. This can be particularly important in limiting liability for the use of a stolen debit card.

17. Carefully examine all medical bills and statements for services that you receive to make sure that medical charges are not being made for services received by someone else using your medical insurance.

18. Never give personal information on the phone to someone you have not called. You never can be sure of the identity of a telemarketer or anyone who solicits you on the phone.

19. Protect your computer with a proper firewall and with security software that automatically is updated.

20. Protect your smartphone or other portable electronic devices with security software and good passwords.

21. Shred, shred, shred any documents that you intend to discard that have any personal information on them. Make sure you use a cross shredder because straight-shredded material can be reconstructed by identity thieves. Although the IRS has up to six years in which to audit your income tax return if they allege you underreported your income by at least 25%, you are probably safe shredding income tax returns and supporting records after three years, the normal period for the IRS to perform an audit. Credit card statements, canceled checks, and bank statements should be shredded after three years.

22. When doing any financial transactions on your computer, laptop, or smartphone, make sure that your communications are encrypted. This is particularly important if you are using public Wi-Fi.

23. Don't share your passwords with anyone, and make sure you use complicated passwords that are not something easily identified with you, such as your pet's name.

24. Limit the information you share on social networking sites in order to make it more difficult for identity thieves to access your personal information that can be used to make you a victim of identity theft.

25. I know it is boring, but read the privacy policies of any Web sites you go to on which you provide personal information. Make sure you know what they do with your personal information, whether they share it with anyone, and how they protect it. What you read might surprise you, and it might influence you to avoid that Web site.

26. Not all of your personal information is on your computer and not all identity thieves come from Nigeria. Sometimes they are relatives, neighbors, or anyone else who might have access to your home and access to your personal records that might contain your Social Security number or other important information. Keep your personal and financial information documents locked and secure at home.

Credit Cards - Becoming less vulnerable

Identity thieves believe that they deserve a lot of credit. Unfortunately, the credit to which they are convinced they are entitled is yours. Credit cards present an all-too-easy target for identity thieves. Protecting your credit cards from identity theft should be a priority for everyone. Take the following steps to reduce your chances of being the victim of credit card fraud:

1. Sign your credit card as soon as you receive it, and activate it. Some people believe that instead of signing your credit card, you should write “See ID” on the signature line on the back of the card. The hope is that whenever your card is used, the clerk or whoever is processing your purchase will check your ID to make sure that you are the one using your credit card. It sounds like a good idea, but credit card issuers are in general agreement that it is best to sign your card. Under the rules enforced between merchants and the major credit card issuers, such as Visa, MasterCard, and American Express, a merchant is supposed to compare the signature on the sales slip with the signature on the credit card. The merchant should refuse to go through with the transaction if the cardholder refuses to sign his or her card.

2. As much as possible, do not let your credit card out of your sight when you make a purchase; a significant amount of credit card fraud occurs when the salesperson with whom you are dealing, out of your view, swipes your card through a small apparatus called a “skimmer” that gathers all the information embedded in your card. The thief then uses that information to make charges to your account. Skimmers can also be unobtrusively installed on ATMs, gas pumps, and any other machine through which you swipe your card. Always check any ATM or other machine for tampering before inserting your card.

3. Save your receipts and ultimately destroy those receipts by shredding. 4. Never give credit card information over the phone to anyone unless you have initiated the call.

Online Shopping Credit Card Protection

The opportunities for identity theft during online shopping are magnified. Two ways of reducing the odds are through the use of either a single-use card number provided to you by your card issuer or by the establishment of a password to be used when your credit card is used online.

The single-use authorization number is tied to your credit card, but has a distinct one-time effectiveness so that even if the number is compromised, your credit remains safe from identity theft. Even less bothersome to a regular online shopper is the use of a password that you set up with your credit card issuer.

When you enter your credit card number during an online purchase, a pop-up box will appear, requesting your password. After you enter the password, the transaction continues. As further security, the Internet retailer with which you are dealing never sees or has access to your password. So even if the retailer's security is breached, your

credit card is safe. More and more people are doing their online shopping on their smartphones and other portable devices.

Unfortunately, many people are not vigilant in protecting the security of their smartphones and portable devices through proper updated security software, and identity thieves are well aware of this fact. One way that identity thieves get access to your smartphone is through corrupted free apps that you download that contain keystroke-logging malware that can read all the information contained in your smartphone or other device, including credit card numbers.

Tip

Download apps only from official app stores such as iTunes. Even then, read reviews before downloading them, and make sure that your smartphone and other personal electronic devices are properly protected with regularly updated security software.

Protect Yourself from Identity Theft at the ATM

Automatic teller machines are a great convenience, but they also present a significant risk of identity theft. Here are a few tips you should follow to prevent an ATM from turning into an identity thief's jackpot paying slot machine:

1. Avoid privately owned ATMs. Whenever possible, use ATM machines of your own bank. This not only saves you from an increased danger of identity thievery, but also lowers the fees you would otherwise pay for merely accessing your own bank account.
2. Take a careful look at any ATM you are using for indications that its exterior has been tampered with.

3. Look around for hidden cameras. Banks themselves will have cameras, but they are generally embedded in the ATM itself.

Mailboxes and Identity Theft

Most mailboxes come equipped with small red flags that when raised indicate that the owner of the mailbox has outgoing mail to be picked up by the mailman. They also can serve as an invitation to identity thieves to raid your mail. An old-fashioned, but still viable, form of stolen mail identity theft occurs when your mail, containing checks to creditors such as credit card companies or your mortgage payment, is grabbed by an identity thief.

The thief performs a process known as “check washing” through which the amount of the check and the name of the payee is changed from the person or business to which you made out the check to the name of the identity thief. Common household cleaning products

such as bleach can be used to “wash” the check and remove the name of the payee. The check is then rewritten payable to the identity thief in an amount of the thief’s choosing.

It is not just your outgoing mail that is fodder for identity thieves. Mail left in your mailbox by the mailman can include new credit cards, Social Security checks, income tax refunds, credit card applications, and credit card statements, as well as other documents that can be utilized for identity theft purposes.

Tips

- When mailing checks, mail them directly from the post office. Or better yet, try secure online bill paying. As for incoming mail, you might consider a locked mailbox or a post office box at the post office.
- If a credit card bill or bank statement is late in arriving, it might mean that your identity has been stolen and the identity thief has changed the address of the account. Always be vigilant in keeping track of the timely receipt of all financial account documents and bills.
- When ordering new checks, don’t have them mailed to your home, where an identity thief can steal them from your mailbox. Pick them up yourself at your bank.

- Never click on any link from a source you are not totally convinced is legitimate. In this case, the United States Postal Services does not send e-mails for unclaimed packages. In any event, if you have any concerns about the legitimacy of such an e-mail, telephone the entity at a phone number that you know is accurate to determine whether the e-mail is a scam.

Job Scams

Many people search online for jobs through a number of legitimate Web sites including Monster.com. Unfortunately, although Monster.com and many other companies try to monitor their job postings for legitimacy, they do not and cannot guarantee that scammers and identity thieves will not be there.

Tip

Never include your Social Security number or too much identifying personal information on your resume. Often identity thieves will request personal information for a routine background check. Never provide such information until you have checked out the company to make sure that it is legitimate and that the person contacting you allegedly representing the company is legitimate. Identity thieves

might ask for your bank account number in order to make a direct deposit of your salary.

Don't give this information or any other personal information to a potential employer until you have confirmed not only that the company itself is legitimate, but also that you are not dealing with an identity thief who says he is with a legitimate company. A quick call to the legitimate company's HR department can provide the information you need to make a good decision.

Danger Where You Never Would Expect It

Most copy machines are complex pieces of machinery that since 2002 have contained hard drives that permit scanning, storing of documents, and other high-technology functions. Unfortunately, when you make a copy on such a machine, whatever you have copied remains on the hard drive, so if you were to copy an income tax return on a public copy machine, your personal information would be stored on the computer's hard drive, available to enterprising identity thieves who buy used copy machines.

When the Federal Trade Commission became aware of this problem, it notified copy machine manufacturers, and since 2007 all copy machines have been equipped with technology that either encrypts

the data on the hard drive or provides for its erasure. Unfortunately, for copy machines manufactured between 2002 and 2007, this problem still exists. Tip Check the date of any copy machine you might use, and if it predates 2007, do not use it for copying documents with personal information that can make you a victim of identity theft. The easiest way to check on the date of the copy machine is to look at the instruction manual.

More Tips for Making Yourself Safer from Identity Theft

1. Consider paying bills online. It can be cheaper and more secure. But be sure that the online service you are using has security protection. Anytime you provide personal information online, make sure that the site is secure. On Internet Explorer, look for the little lock symbol which shows that your information is being encrypted.

2. Check your bank statements, telephone statements, credit card statements, and brokerage account statements for unauthorized charges. Each month when you get your statements, scrutinize them carefully to make sure that every charge is legitimate. Keep your statements in a safe and secure place. Shred the statements when you no longer need them. If a monthly bill does not arrive on time, promptly notify the company. Sometimes a thief will use your personal information to get your credit card company or other

company with which you do business to send your bill to a new address. In this way, the identity thief is able to prolong the period that he or she is able to fraudulently use your account before you or the company becomes aware of its improper use.

3. Your mother was right. Don't talk to strangers. Updating Mom's advice, don't talk to strangers online. Do not download files that are sent to you from people you do not know. Not only could your computer be damaged through a virus, but you also could be subjected to computer programs commonly called "spyware" that permit an identity thief to access your personal information.

4. Do not carry your Social Security card in your wallet.

5. Get a shredder to destroy all your unnecessary financial records as well as preapproved credit card offers. Dumpster-diving identity thieves can go through your trash to find the mother lode of information for identity theft.

6. Do not write down your PIN or passwords. However, be sure that whatever PIN or password you choose is not something that is easily associated with you, such as your name or your pet's name.

7. Do not store your personal information on your laptop computer. Laptop computers present a tantalizing target for thieves. Many people prepare their income tax returns on their computers,

forgetting about the sensitive personal financial information that might be left on their hard drives. Always remove this information from your computer upon completion of your tax return.

8. Get a good antivirus software program and keep it constantly updated. Viruses can infect your computer with spyware programs that, unbeknown to you, might cause your computer to send information stored on your computer to the hacker that can facilitate identity theft.

9. Set up a firewall on your computer. A firewall is a computer program that makes it more difficult for hackers to get access to your computer by preventing or selectively blocking access to your computer through the Internet There are many good firewall programs that are easy to install on your computer.

10. When you get rid of your computer, it is not enough to merely delete personal information. Deleted information remains on your hard drive and can be readily accessed by a computer-savvy identity thief. Make sure you use one of the special programs, such as the free program Eraser, that will effectively remove the information from your hard drive. Alternatively, you can do what I prefer to do, which is remove the hard disk from the computer and smash it into oblivion with a hammer.

11. Take advantage of obtaining your annual free credit report from each of the three credit-reporting agencies— Equifax, Experian, and TransUnion— so you can look for unauthorized charges and evidence of identity theft, as well as make sure there are no innocent mistakes on your reports that could harm your credit. Obtain your free credit reports on a staggered basis from each of the three credit-reporting agencies and get one every four months for better, more current protection. You can get your report from Equifax at www.equifax.com, from Experian at www.experian.com, and from TransUnion at www.transunion.com.

12. Put a credit freeze on your credit report at each of the three credit-reporting agencies. Through a credit freeze, you are able to prevent access by anyone to your credit report even if they have your Social Security number. You are the only one who has access to your credit report, by way of a PIN that you pick. If you need to apply for credit, you can temporarily lift the freeze on your credit report and then put it back when the company you want to have access to your report has finished.

13. If you are in the military and deployed away from home, you can place an active duty alert on your credit reports at each of the three credit-reporting agencies that lasts for a year and can be renewed if necessary. This will restrict access to credit without your approval.

Protecting yourself online

1. Install good security software to protect your computer from viruses, spyware, and other malware. There are many legitimate companies that offer free security software, but make sure that you are dealing with a reputable company and consider paying for a product that will provide you with greater protection.

2. Keep your security software up-to-date. Automatic updates are best.

3. Encrypt the data on your laptop. Microsoft's BitLocker will do the job free; however, it is available only with Windows 7. TrueCrypt is another free encryption service that will protect the data on your computer from prying eyes in public.

4. Use strong, difficult-to-guess passwords.

5. Never turn off your firewall. Firewalls maintain a protective barrier between your computer and the Internet.

6. The price of computer security is eternal vigilance along with a healthy dose of mistrust. Never download anything from a source that you do not absolutely trust, and even if you trust the source—don't. First communicate with the source to make sure that the material you are being asked to download or link to is actually from

that person or company that you trust, and even then, remember that they could have been compromised and could be unintentionally sending you corrupted material.

7. Regularly get, and review for accuracy and signs of identity theft, a copy of your credit report. You are entitled by law to get a free copy of your credit report annually from each of the three major credit-reporting bureaus, Equifax, Experian, and TransUnion. The most efficient way to do this is to request a copy in sequence from one of them every four months. This way you stay more current in your review of your credit report, at no cost. It is also important to remember that there are a number of services that will lead you to think that you are ordering a free credit report from them, but in the fine print you will find that you have signed up for a continuing costly service that you might not need or want. The only place to get your truly free credit report is www.annualcreditreport.com or by phone at 877-322-8228.

8. If you are in the military and are deployed overseas, you can request that an active duty alert be put on your credit report that will not permit credit to be issued without your specific approval for a year. The active duty alert can be extended after the first year for additional years. You can also designate a personal representative

here in the states to give approval on your behalf if you are applying for credit while overseas but can't be reached.

What If You Become A Victim of Identity Theft

Don't feel too bad if, despite your best efforts, you become a victim of identity theft. You are in good company. The list of prominent victims of identity theft includes Oprah Winfrey, Michael Jordan, Tiger Woods, Steven Spielberg, Ted Turner, Warren Buffet, New York City Mayor Michael Bloomberg, Robert DeNiro, Martha Stewart, Will Smith, and Ross Perot. Fortunately, there are some steps you can take to respond to the theft of your identity and to minimize the damage:

1. Put a fraud alert on your credit report. If you think that you might be the victim of identity theft, you can have a fraud alert placed on your credit report at the credit-reporting agencies. The alert stays on your report for up to 90 days but can be extended for up to seven years. When a fraud alert has been put on your credit report, you are entitled to a second free credit report during that year in order to monitor your credit for further irregularities. In the past, people placing a fraud alert on their credit reports found that for it to be effective, they had to call each of the three major credit-reporting agencies to have fraud alerts independently placed on each

company's record. Now, under FACTA (the federal Fair and Accurate Credit Transactions Act), all you need to do is call one of the credit-reporting agencies and they are required to notify the other two to place the fraud alert on your file. Unfortunately, fraud alerts are not always as effective as you might think. The law does not require businesses to check for fraud alerts before granting credit, and there are no penalties for companies failing to monitor credit reports for fraud alerts. Many companies do not even bother to check for fraud alerts, and due to technical procedural problems, notifying one of the credit-reporting agencies to place a fraud alert might not result in a fraud alert being placed on your credit report at the other two credit-reporting agencies.

2. A better solution might be to place a credit freeze on your credit report. This sendee, available in all states, permits you to effectively seal your credit report from access by anyone (such as an identity thief with your Social Security number and other personal information) without the use of a PIN that you pick to make your credit report available. Thus, an identity thief is prevented from using your credit report to secure credit or open a new account in your name. Consumers Union has a very user-friendly Web site that can help you access the credit-freeze law for your particular state by going to www.consumersunion.org/campaigns/learn more/oc>3484indiv.html# MA. Even if you have not been a victim of

identity theft, a credit freeze is a great preventive measure to take to protect yourself from identity theft.

3. Go to the Federal Trade Commission Web site to obtain the FTC's ID Theft Affidavit, and use it to report the crime.

4. Contact all your creditors by phone and then follow up with a letter sent by certified mail, return receipt requested. Get new credit cards with new account numbers. Change your PIN and your passwords.

5. Close tainted accounts. When opening new accounts with these creditors, use a password that is not easily connected with you. A word to the wise: Do not use your mother's maiden name, or to be particularly safe, do not even use my mother's maiden name. People think that their mother's maiden name is difficult to find. It is not. It is on your birth certificate, a public record.

6. When you close accounts, make sure that the accounts are designated as being closed at the customer's request due to theft so that when information is transmitted to the credit-reporting bureaus, it is clear that the problems are not of your doing.

7. Ask your creditors to notify each of the credit-reporting agencies to remove erroneous and fraudulent information from your file.

8. If your checks are stolen, promptly notify your bank and have the account closed immediately. If your checking account is accessed by checks with forged signatures, you obviously have not authorized the withdrawals and should not be held responsible for money stolen from your account. However, if you neglect to monitor your account and fail to promptly notify your bank when there is an irregularity in your account or your checks are lost or stolen, you might be held partially responsible for your losses. It is not even necessary to have your checks physically stolen for you to become a victim. An identity thief armed with your name, checking account number, and bank routing information can use one of a number of inexpensive computer software programs to create checks for your account.

9. Contact the various check-verification companies and ask that they, in turn, contact retailers who use their services, telling them not to accept checks from your accounts that have been accessed by identity thieves.

Check-verification sendees are companies that maintain databases of bad check writers. Retailers using their sendees contact the verification sendee's database before accepting checks. Among the companies that do check verification are CellCharge, CheckCare, and CrossCheck.

10. To see whether checking accounts have been opened in your name, contact ChexSystems at www. consumerdebit. com to request a free copy of a report that lists all checking accounts in your name. If you find that an account has been opened in your name, contact the bank and instruct them to close the account.

11. File a report with the police both where the fraud occurred and where you live. You might find police departments reluctant to accept your report, sometimes for technical legal jurisdictional reasons. Politely insist that they at least accept your report. Remind them that credit bureaus will prevent fraudulent accounts from appearing on your credit report if you can provide a police report. Give the police officer taking the report as much documentation as you have to support your claim, including the ID Theft Affidavit approved by the Federal Trade Commission that appears later in this book. When a police report has been filed, send a copy of it to each of the three major credit-reporting agencies.

12. Be proactive. Contact your creditors where you have tainted accounts and get a written statement from each of them indicating that the account accessed by an identity theft has been closed and that the charges made to the accounts are fraudulent. Request that they initiate a fraud investigation. Find out what you are required to do to advance the investigation, such as providing them with a

police report. Remember to get a written copy of your creditor's completed investigation.

13. Send copies of your creditors' completed investigations to each of the three credit-reporting agencies. Ask them to send you a copy of your updated credit report in order to confirm that any erroneous and fraudulent information has been removed from your file.

14. If fraudulent charges do appear on your credit report, notify the credit-reporting bureaus in writing that you dispute the information and request that such information be removed from your file.

15. If you are contacted by a debt collector attempting to collect a debt incurred by an identity thief in your name, write to the debt collector within 30 days of receiving the initial notice from the debt collector. Tell the debt collector that the debt is not yours and that you are a victim of identity theft. Send a copy of the identity theft report, police report, or other reports you might have completed. After you provide this information, the debt collector is required by law to cease collection efforts until they have verified the accuracy of the debt. Additionally, you should also contact the company for which the debt collector is attempting to collect the debt and explain

to them that the debt is not yours, but rather is the result of identity theft. Also, ask them to provide you with details about the transaction creating the debt, including copies of documentation that might contain the signature of the identity thief. Finally, contact the credit-reporting agencies and ask that they block the incorrect information from appearing on your credit report.

16. If your driver's license is possibly in the hands of an identity thief, you should cancel the license and get a new one.

17. If your passport is lost or stolen, contact the State Department at www.travel.state.gov/passport to arrange to get another passport and to have it recorded that your passport has been lost or stolen.

18. If your mail has been stolen and used to make you a victim of identity theft, the Postal Sendee will investigate the crime. Notify the postal sendee at your local post office.

19. If an identity thief has used your identity to set up phony accounts for utilities such as phone, cable, electricity, or water, contact the utility provider and report the crime. Provide them with a copy of your identity theft report and close the account. You should also contact your state public utility commissioner's office and inform them about the crime and provide them with your identity theft report so that they can investigate this as well.

20. If your information has been used to obtain a student loan in your name, contact the school or the lender, provide them with the identity theft report, and ask them to close the loan. You should also report the crime to the U.S. Department of Education at www.ed.gov/about/offices/list/oig/hotline.html.

21. If your Social Security number has been misappropriated by an identity thief, contact the Social Security Administration at

www.socialsecurity.gov, or by phone on their fraud hotline at 800-269-0271, or by mail at Social Security Administration Fraud Hotline, P.O. Box 17785, Baltimore, MD 21235.

Stop Identity Theft at work

The workplace is a good place to make money, particularly if you are an identity thief. Here are some basic steps to take to help prevent your workplace from becoming a profit source for an identity thief:

1. Anyone who has access to your workspace might have access to your computer and the information contained therein. Fellow workers, visitors, business support personnel, or, at worst, burglars can get at the information in your computer unless you protect it. Use passwords for sensitive information. Turn off the computer

when you are not using it, or set the computer to automatically log out after a few minutes of nonuse.

2. Use encryption programs.

3. Do not have your passwords stored in your software for frequently visited Web sites. Log them in each time you visit a site. You might want to change your password periodically. If you do, mix letters and numbers to make your password less vulnerable. And, of course, it is important to have passwords you can remember.

4. When you replace your computer, make sure that the hard drive on your old computer has all the information stored there permanently erased. Merely deleting information on your computer does not permanently erase data. There are various inexpensive software programs that will permanently remove information from your hard drive.

Tips for Protecting Your Social Security Number

Maintaining the privacy of your Social Security number is the single most important thing you can do to help protect yourself from becoming a victim of identity theft. Here are some tips to follow:

1. Don’t carry your Social Security number with you in your wallet or purse. Keep it in a secure location.

2. Even when asked for your Social Security number by a company or an agency, ask whether they will accept an alternative identifying number, such as your driver's license. Many will understand and comply with your wishes.

3. Don't write your Social Security number or have it printed on your checks, address labels, or any other circulated item.

4. Make sure that you order your free copy of your credit report from each of the three major credit-reporting agencies each year at www.annualcreditreport.com. This will enable you to see whether your Social Security number has been compromised or whether there are any other Social Security numbers associated with you.

5. As odd as it might seem, limit sharing your birthday, age, or place of birth online, particularly on social media. A study done at Carnegie Mellon University in 2009 found that to a significant degree, a person's Social Security number can be guessed based on this information. The Social Security Administration for a long time assigned Social Security numbers partly based on geography. Particularly for people born since 1989, when Social Security numbers began being assigned shortly after birth, it is relatively easy to predict a person's Social Security number. And it also makes

it easier for an identity thief who knows the first five digits to trick a victim into providing the remaining digits through phishing or some other scheme. It also is easy for an identity thief to use botnets to send out thousands of applications for credit with various guesses at your Social Security number until he or she hits the right one. Fortunately, since 2011 the Social Security Administration started assigning Social Security numbers randomly. But for anyone reading this book, your Social Security number remains the same and you should be aware of the risks.

What to do if you are the victim of a criminal identity theft?

1. Act as soon as you become aware of the problem. Hire a lawyer and contact the police and the District Attorney's office to straighten out the matter. File a report indicating that you are the victim of identity theft. It will be necessary for you to confirm your own identity through photographs and fingerprints. In addition, show law enforcement authorities your driver's license, passport, or any other identification that you might have that contains your photograph.

2. Get a letter from the District Attorney explaining the situation to have available if you are ever stopped for a traffic violation and your record is checked. The states of Arkansas, Delaware, Iowa,

Maryland, Mississippi, Montana, Nevada, Ohio, Oklahoma, and Virginia have Identity Theft Passport Programs. Through these programs, anyone whose identity has been appropriated by someone who uses it in the commission of a crime can, upon proving their identity, receive an Identity Theft Passport. The Identity Theft Passport protects them and confirms their true identity if there is a question about their criminal responsibility. Even if your state does not have an Identity Theft Passport program, obtain from the law enforcement agency that arrested the person using your name a "clearance letter" or "certificate of release" which indicates that you have not committed the crimes that were the subject of the arrest of the identity thief who used your name. Keep these documents with you at all times.

3. Make sure your criminal record is expunged.

4. Consider changing your name.

5. Consider changing your Social Security number.

Tax Filing Tips

Income tax fraud has become a huge problem, but there are things that you can do to minimize the chances of your becoming a victim of income tax fraud. Here are some things you should consider:

l. Protect your W-2 and other forms with personal information that you need in order to prepare your income tax return, but can result in your becoming a victim of tax identity theft if the forms fall into the hands of an identity thief.

2. If you decide to have your income tax return prepared by a professional tax preparer, make sure that you have carefully verified that the tax preparer is legitimate. In addition, even if you choose an honest tax preparer, their computers can be hacked and can make you a victim of tax identity theft too. So ask them what steps they take to protect the security of your information in their computers and in their files.

3. If you are e-filing on your own, make sure that you use a strong password. After you have filed, it is a good idea to put the tax return on a CD or flash drive that you keep in a secure place and then remove the information from your computer's hard drive. This will protect you if your computer is hacked.

4. If you are e-filing on your own, make sure that your firewall and security software are current.

5. If you use regular mail to file your income tax return, mail it directly from the post office rather than leaving it in a mailbox from which it could be stolen.

6. If you are getting a refund, you should consider having your refund sent electronically to your bank account rather than having a check that can be stolen sent to you through the mail.

7. File early. Identity thieves file early to steal your refund before you have a chance to file.

Steps to Take If You Are a Victim of Tax Identity Theft

If despite your best efforts, you have become a victim of tax identity theft, you should promptly take the following steps:

1. File a report with the Federal Trade Commission's identity theft database.

2. Call the Federal Trade Commission's hotline for personal identity theft counseling at 877-ID-THEFT (438-4338).

3. Put a credit freeze on your credit report with each of the three major credit reporting agencies.

4. Call the Identity Protection Specialized Unit of the IRS at 800-908-4490-

5. File an IRS Identity Theft Affidavit Form 14039 with the IRS.

Identity Theft Insurance

From high-technology biometrics to low-technology identity theft insurance, the recognition by businesses and government that identity theft is a problem that must be dealt with in as many ways as possible is a good development.

In response to the problems presented by identity theft in recent years, the financial industry has developed identity theft insurance. Generally, these policies are not used to reimburse you for money that might have been stolen from you through identity theft. Instead, they will help pay for the costs involved with correcting the problems that come with identity theft, such as fixing your credit report and lost wages due to taking time off from work due to the time and burden involved in repairing your credit.

Some homeowners' or renters' insurance policies provide as much as $25,000 of coverage for identity theft for little or no additional cost. A number of major insurance companies also offer separate identity theft policies for relatively small annual premiums of between $25 and $195. Finally, many credit cards offer identity theft protection as an optional benefit for cardholders, some at no cost. Some card issuers provide the insurance to all their credit card customers, whereas others provide it either as an additional benefit

of their premium cards or as an inducement to new customers to apply for the particular card providing this benefit.

But regardless of how little the premium might be, do you really need the coverage? Generally, you are not responsible for unauthorized charges beyond $50, and most companies do not even hold you responsible for that amount. The real cost of identity theft for many people is the cost of the time it takes to have their good name and their good credit restored.

In addition to being sold by credit card companies, stand-alone identity theft insurance is sold by insurance agents, credit bureaus, identity theft protection companies, banks, and credit unions. The better policies will monitor multiple sources of information for signs of identity theft, such as your credit report, public records, and even black market Web sites where identity thieves buy and sell personal information.

Factors to Consider When Buying Identity Theft Insurance

Not everyone needs identity theft insurance; however, for some people, the cost and convenience might make its purchase a wise choice. However, not all identity theft insurance policies are the

same. Here are some things you should consider before buying identity theft insurance:

1. What sendees are provided? Does the policy provide assistance with resolving identity theft or does it merely compensate you for costs you incur in remedying the problem?

2. Is there a deductible? Deductibles of $500 or more can reduce the value of the insurance to you if the company is reimbursing you only for your out-of-pocket costs.

3. Does the policy cover legal expenses? Not all policies do.

4. Does the policy cover lost wages in regard to time lost from work while you are correcting the problems caused by identity theft? Again, not all policies cover lost wages.

It is important to remember that despite the impression given by some advertising, identity theft insurance does not prevent identity theft, but more often merely makes you aware of identity theft sooner than you would have on your own.

In fact, LifeLock, one of the most prominent identity theft insurance companies, settled false advertising charges with the FTC and a group of 35 state attorneys general by agreeing to pay $12 million. LifeLock's advertising implied that it could offer absolute protection against identity theft. The fraud alerts that LifeLock placed on its

policyholders' credit reports were of limited use in preventing identity theft, and nothing LifeLock did provided any protection against medical identity theft or employment identity theft. Perhaps even more disturbing was the charge by the FTC that LifeLock gathered sensitive personal information about its customers, but did not, despite its claims to the contrary, encrypt the data, making its own data a good source of information for potential identity thieves.

If you do opt for an identity theft insurance policy, look for one with a low deductible that also will provide for payment of legal fees, which can be considerable if an identity thief commits crimes in your name. You might decide that through the use of a credit freeze, which is infinitely superior to a fraud alert, you can protect your credit report better and more cheaply on your own than through identity theft insurance. You might also decide that by staggering your free annual credit reports from the three major credit reporting agencies—Equifax, TransUnion, and Experian—you can get one free report from one of them, and then four months later a free report from a second one, and then four months later a free report from the third credit reporting agency, and monitor your credit report far more cheaply than through the purchase of identity theft insurance.

Protecting Your Privacy—A Key to Preventing Identity Theft

A key to preventing identity theft is limiting the exposure of as much data about you as possible. Identity thieves exploit the availability of personal information from free Web sites throughout the Internet as well as by hacking into the companies and agencies that hold personal information about us. Unfortunately, not enough of us consider this even though we know that the more places that have information about us, the greater the possibility of identity theft occurring through hacking and other actions over which we have no control. According to Consumer Reports, almost half of the victims of identity theft in 2011 became victims not because of their own actions, but because their personal information had been stolen or hacked from companies, government agencies, and others who store our personal information. Regardless of how vigilant you are about protecting your privacy, your information is only as safe as the many places which store that information. As my grandmother used to say, “I can keep a secret; it is the people I tell who can’t keep a secret.”

Privacy Settings on Facebook

Facebook, by its very nature, is a place for sharing information; however, as the figures provided by Consumer Reports indicate, few people are aware of or exercise their rights to limit their information on Facebook by consciously utilizing its privacy settings. For each of the settings on your Facebook account, you can set your privacy settings to share the information with everyone, your network and friends, friends of friends, or only friends. You should deliberately determine what information you want to share and with whom. Personal information such as your birth date, place of employment, and the names of relatives can be used by identity thieves to help make you a victim of identity theft. Sharing information with friends of friends could expose your data to large numbers of people whom you might not want to have your information.

To limit access to some of your profile information, such as your birth date, relationship status, or employer, all you need to do is click on the Update Info button in the box below the Timeline cover photograph, which will take you to where you can restrict access as you like.

It is important to remember that your Facebook name and profile photograph will always be available to anyone. For greater privacy, some people choose a profile photograph that is not of their face.

You also can use a different name from your real name as your Facebook name for increased privacy.

If you are among the people who have never used the privacy settings, most likely all of your status updates have been set to Public by default. You might want to go through your posted personal information and limit the audience for the items you would prefer to restrict.

Unwittingly, your friends might share information about you with identity thieves. Without your knowledge or your friend's knowledge, an app that they use could get access to your information. Fortunately, however, you can prevent this by turning off all apps, which will prevent all apps your friends use from being able to gain access to your information. However, this Draconian action will also prevent you from being able to use any games, apps, or other sites available on Facebook. If you want to follow this course of action, you should go to the Home section and bring down a menu to your Privacy Settings and click the Edit Settings link in the Ads, Apps and Websites area. Next you should click the Turn Off link to turn off all apps. Alternatively, you can take the less drastic step of merely restricting the information you share with apps and selectively determining what information you want to share with apps used by your friends. You do this by going to your Privacy

Settings and clicking the Edit Settings link in the Ads, Apps and Websites area. Then go to How' People Bring Your Info to Apps They Use and click the Edit Settings button. There you can limit various information such as your biography, birth date, family and relationships, hometown, current city, education, and work.

To create an app for Facebook, all you need is a Facebook account, a cellphone number, and a credit card. Identity thieves can certainly supply all of that.

You might want to regularly check your Facebook page to see how it appears to others and perhaps adjust your privacy settings. The way you do this is to click on your username at the top of your Home page to go to your Timeline page. Then click Update Info. This will show you what other people see when they go to your page. If you want to see how your Facebook appears to a particular person, you can enter your friend's name in the box there. If you find that there is information that you do not want to make available to that particular person or others, you can remedy this by changing your privacy settings. To do this, merely go from your Home page to the Home tab at the top right of the page and then click the arrow' to the menu and go to Privacy Settings. There you can restrict or block information generally or in regard to particular people.

It is important to remember that it is up to you to take action to protect your privacy on Facebook. Because of Facebook's business model, the more information it provides its advertisers, the more advertising dollars it pulls in. Facebook's interests in profits do not necessarily coincide with what might be your desire for privacy.

Protecting Your Privacy on Google

Most Web sites and search engines, such as Google, Yahoo!, and Bing, use cookies. Cookies track your Internet usage and the Web sites you go to. They are used by search engines to tailor advertising to your interests; however, they also can be used by identity thieves to produce more enticing phishing Web sites. If you do not want to receive cookies when you go to Google, you can change your browser's setting to refuse cookies in general or from specific Web sites.

Dangers of Data Gatherers

With so much personal information available on the Internet, companies have arisen that gather this information and for fees of between $2 and $50 provide anyone who asks and is willing to pay for it with your name, address, age, telephone number, home's value

if you own one, previous addresses, previous criminal comictions, educational background, occupation, hobbies, and more. These data-gathering companies primarily provide this information to advertisers, because the more they know about you, the more they can efficiently target specific advertising to your own preferences. But this information can also be misused by identity thieves, making it easier for them to trick you into providing the remaining information they need in order to make you a victim of identity theft.

For those who are particularly security-conscious, there are many companies that will provide you with greater security while you use the Internet and prevent data collectors from following you online. Some of the popular ones are Abine, AdBlock Plus, Disconnect, and Do Not Track Plus. Abine has a free version and other versions for $3 per month or $99 per year that will let you block cookies. Unfortunately, it wrorks only with Mozilla Firefox and Internet Explorer browsers at the present time. AdBlock Plus is free and blocks out all advertising. It is available only for the Mozilla Firefox browser. Better Privacy is free and prevents hidden flash cookies from storing information about you, but it too works only with Mozilla Firefox. Disconnect blocks both ads and social network tracking. It also permits you to use Google without being tracked.

Finally, Do Not Track Plus is also free, blocks out advertising, and is available for Mozilla Firefox, Chrome, Internet Explorer, and Safari.

Do Not Track

Many people are pushing for a federal law that would require Web sites and browsers to tell you when you are being tracked and to provide a Do Not Track List for which you could enroll, similar to the Do Not Call List to stop telemarketers from calling you. Passage of such a law in the short run is not likely.

However, unbeknownst to many people who use Internet Explorer 9 and Mozilla Firefox 5 as Internet browsers, both of these browsers already provide Do Not Track capabilities that take no more effort than just choosing it as an option on your toolbar. Primarily because most people aren't aware of this important option, only about 1 percent of Internet Explorer 9 and Mozilla Firefox 5 users have chosen this option.

Steps to Take to Increase Your Privacy

There are several affirmative steps we can take to increase our privacy and make us less susceptible to identity theft. Here are some of the most important ones:

1. The credit-reporting agencies regularly sell our names and addresses to other businesses that will solicit your business. You can prevent your name and address from being sold by the credit-reporting agencies to other businesses by calling 888-5OPTOUT (567-8688). Among other things, this will have you taken off of the lists for the so-called “preapproved” credit cards, which pose a particular danger of identity theft if the mailing is intercepted by an identity thief.

2. To be taken off of the Direct Marketing Association’s own list, which is the source of much of your junk mail, go to

www. dmachoice. org/dma/member/regist. action, where you can first register your name and address and then have it placed on a “do not mail list." There is no cost to register or to be placed on the “do not mail list."

3. If, like many of us, you have ever purchased something through a catalog, your information has been shared with other catalog companies through a company called Abacus. You can, however, opt out of the Abacus database and prevent more catalogs from being sent to you by sending an email to abacusoptout@epsilon.com in which you provide your name including your middle initial, your current address, and a request to be removed from their database

4. Don't fill in product registration cards that you get when you purchase consumer goods. The implication is that you need to complete the cards and return them in order to be covered by warranties for the particular goods you have purchased, but that is not the truth. You do not need to register to be covered by a product's warranty. Failing to return the card does not negate your warranty. Your receipt is good enough evidence of the purchase of the particular goods should you need to exercise your warranty rights. However, for products such as car seats, cribs, or other products that might potentially be subject to a safety recall, you might want to return the card so that you can be notified in the event of a recall. In this instance, you should provide only your name, your address, the date of purchase, and the product serial number.

5. Carefully evaluate your privacy settings on your social network sites and set them up at a level with which you are comfortable.

6. Use the Do Not Track option for Internet Explorer 9 and Mozilla Firefox 5 for your Internet browsing.

Identity Theft and the Elderly

The elderly are often particularly targeted for identity theft. Identity theft and fraud against the elderly is a particularly insidious problem because, in many instances, when the senior realizes that he or she has been scammed or made the victim of identity theft, he or she is often hesitant to report the crime out of embarrassment or shame and the belief that it is just another example of their losing their mental acuity. In fact, anyone can be scammed or can be a victim of identity theft. Very intelligent people were scammed, for instance, by Bernie Madoff. A recent study by MetLife has shown a dramatic increase in scams perpetrated against people over the age of 60 in the past few years and the problem is getting worse.

The elderly are also often targeted because they have savings and pensions that can provide easy pickings for identity thieves. The elderly, as a group, are more likely to have good credit scores and are less likely, on their own, to apply for more credit, so stealing their identity provides more potential for financial gain. Unfortunately, often the people stealing the identities of the elderly are members of their own family, friends, or caregivers. There have been many instances in which rogue nursing home employees have stolen the identities of the residents of the nursing homes where they work if the facility does not properly protect the residents' personal information.

The elderly are often lonely or isolated, which can make them more likely to listen to the tale of an identity thief who calls them on the phone. They also might not have people around them to warn them of the dangers posed by identity thieves. According to a survey done by International Communications Research in 2002, more than a third of people over the age of 60 did not even know what identity theft was.

The dependency of many elderly on caregivers, whether professionals or family members, also makes them more vulnerable to identity thieves, whether family or professional criminals.

Medicare Identity Theft Threats

Despite calls from the General Accountability Office (GAO), the investigatory agency of the federal government, Medicare still uses enrollees' Social Security numbers as their Medicare Identification number, and it is also prominently featured on their Medicare Identification card. A common identity theft scam involves seniors receiving calls from telemarketers who contact seniors and tell them that they can receive medical sendees and equipment at no cost by merely providing their Medicare Identification number. A large-scale fraud involving allegedly free supplies for diabetics was used by identity thieves in 2012 to obtain the Social Security numbers of

Medicare recipients; the numbers were then used for making false Medicare claims and for stealing the identities of the Medicare recipients.

Tip

Companies that actually do work with Medicare will not make unsolicited telemarketing calls. In addition, you never should give your personal information, particularly your Social Security number, to anyone who calls you on the phone. You have no way of verifying who they are. If you suspect Medicare fraud, you should call Medicare at their fraud hotline number of 877-486-2048.

Contests and Lotteries

One of the most common scams affecting the public in general, but also preying on seniors in great numbers, are phony contests and lotteries whereby the victims are told that they have won a contest that they have not entered; however, they have to pay certain administrative fees or taxes, as well as provide certain personal information, in order to claim their prize.

Tip

It is hard enough to win a legitimate contest that you have entered. The chances of winning one that you have not entered are nonexistent. Yet by providing personal information to someone who

claims you have won a contest, you can make yourself a victim of identity theft. Never give your personal information on the phone to someone you have not called, and always check out the legitimacy of any contest before providing any information.

How to Help Prevent Elderly Identity Theft

There are many things you can do to help elderly family members or friends become less likely victims of identity theft:

l. Monitor your elderly family members or friends well and often. Caution them against giving personal information to people who don't need it, and make sure their personal information is secure and away from the prying eyes of people who might come to their home.

2. Keep income tax returns in a secure location, and make sure that the person who prepares the senior's income tax return not only is reputable, but also maintains a good security system for protecting the senior's information and records.

3. If the elderly family member or friend is in a nursing home or an assisted living facility, discuss with the management of the facility the security measures that the facility takes to protect the privacy of the personal information of residents.

4. If an elderly family member or friend is in a nursing home, arrange for his or her mail to be sent to you so that you can keep important mail secure.

5. Do not allow caretakers to open mail or deal with any financial transactions on behalf of your elderly family member or friend.

6. Consider handling the elderly person's bill paying online and avoid paper checks that can be stolen and used for identity theft.

7. On behalf of the elderly family member or friend, monitor his or her credit report annually from each of the three major credit-reporting agencies.

8. Register the elderly family member or friend for the federal Do Not Call list to prevent telemarketers from calling; however, recognize that scammers do not comply with the Do Not Call list.

9. To be taken off of the mailing and telemarketing lists, call 800-407-1088. You also can go to the Web site of the Direct Marketing Association at www. dmachoice. org and then go to its FAQ section at the top of the page and click the Do Not Contact for Caregivers link, which takes you to a screen where you can enroll to stop direct marketing advertising from coming to an elderly person in your care.

10. Eliminate preapproved credit card offers, which can be used by identity thieves to get credit cards in the elderly person's name, by going to www. optoutprescreen .com.

11. The credit bureaus sell the names and contact information for the people in their data banks. You can eliminate this as a problem and the junk mail and offers they lead to, which present threats of identity theft when they fall into the wrong hands, by calling 888-567-8688.

12. Shred unnecessary personal and financial records. Many elderly tend to hoard unneeded old records, which can provide fodder for identity thieves.

13. Do not have the elderly family member or friend earn* his or her Medicare or Social Security card. Keep them in a secure place. Snatching of the purse or wallet of an elderly person can give the thief the information necessary to make the senior a victim of identity theft if the purse or wallet contained the person's Medicare or Social Security cards.

14. Put a credit freeze on the elderly family member's or friend's credit report.

15. Check Medicare and medical insurance bills regularly to make sure that there are no improper charges.

Signs of Elderly Identity Theft

If you are looking out for a family member or friend in order to keep him or her from becoming a victim of identity theft, here are some things for which you should be on the lookout:

1. The elderly person has no awareness of a newly issued credit or debit card.

2. The elderly person's checkbook has missing checks.

3. The elderly person's bank account is suddenly overdrawn.

4. Large withdrawals are made from accounts.

5. There is a sudden increase in monthly charges on behalf of the elderly person.

Recap - Identity Theft Protection Rules

Although this list of rules is quite lengthy, in fact, they are not particularly difficult to follow and by doing so, you can go a long way toward protecting yourself from becoming a victim of identity theft:

1. Never give personal information over the phone to anyone whom you have not called, and always be sure of whom you are speaking to.

2. Carry only the credit cards you need to use in your wallet.

3. Never carry your Social Security card in your wallet. Where is that thing, anyhow?

4. If you rent a car, destroy your copy of the rental agreement when you return the car.

5. Consider using a post office box rather than having mail delivered to your home.

6. If you don't use a post office box, use a locked mailbox at your home.

7. Do not bring your checkbook with you on vacation. Use traveler's checks or credit cards.

8. Keep copies of all your credit cards, front and back, as well as the telephone numbers for customer sendee.

9. Remove yourself from marketing lists for preapproved credit cards. If you receive preapproved credit card applications that you do not use, shred them.

10. Sign up for the National Do Not Call List.

11. Check your credit report at least once a year. Because you can get a free copy of your credit report annually from each of the three

major credit-reporting bureaus, stagger your requests so that you get one report every four months.

12. Check your Social Security Statement provided by the Social Security Administration annually.

13. When you get a new credit card, sign it immediately and call to activate it.

14. As much as possible, keep your credit card in sight when you make a purchase to prevent it from being "skimmed."

15. Try paying your bills online, but if you do mail checks, mail them directly from the post office.

16. Check your bank statements, telephone bills, credit card statements, and brokerage account statements monthly for unauthorized charges.

17. Do not download files from people you do not know, and be wary of links that could contain malware even if they come in e-mails from friends, because your friend's e-mail could have been hacked or your friend might unwittingly be sending you tainted e-mail with malware.

18. Shred, shred, and shred all unnecessary financial records and preapproved credit card offers.

19. Do not store your personal information on a laptop computer.

20. Use antivirus software on all your electronic devices and update it regularly.

21. Set up a firewall on your computer and other electronic devices.

22. Remove all personal information from your hard drive when you get rid of your computer, laptop, smartphone, or other electronic devices.

23. Ask any business that has personal information about you about their policy for the protection of that information.

24. Do not use your Social Security number as your driver's license number or on your health insurance card.

25. Do not store the passwords to frequently visited Web sites on your computer. Enter them every time you go to the Web site.

26. Avoid privately owned ATMs.

27. Lock your car and don't leave anything in it that you cannot risk losing.

28. Store your records that contain personal information that could be used to make you a victim of identity theft in a locked, secure place.

29. After you have received a loan, a credit card, or anything else that required you to complete an application containing your Social Security number, request that your Social Security number be removed from the application on record.

30. When doing any financial transactions on your computer, laptop, or smartphone, make sure that your communications are encrypted.

31. Don't share your passwords with anyone, and make sure you use complicated passwords that are not easily guessed, such as your pet's name.

32. Limit the information you share on social networking sites in order to make the work of identity thieves more difficult in regard to getting your personal information.

33. Read the privacy policies of any Web site to which you would provide personal information to find out with whom they share information and how they keep your information secure.

34. Avoid privately owned ATMs.

35. Always check an ATM before you use it for evidence of tampering or the installation of a skimmer. Also look for hidden cameras.

36. When ordering new paper checks, don't have them mailed to your home. Pick them up at the bank.

37. Don't use public copy machines for the copying of your documents that contain personal information such as your Social Security number.

38. Update your laptop before going on any trip on which you will be taking your laptop so that you will not be tempted by infected Internet systems in hotels that might tell you that you need to update your software.

39. When making gifts to charities, don't provide your Social Security number. They do not need it, and it could turn up in publicly available forms.

40. When writing an obituary for a family member, do not include too much information that can be used by identity thieves.

41. Pay your bills online. It is safer than sending paper checks through the mail. Just make sure that the bank's Web site is secure and your computer's security software is updated.

42. Put a credit freeze on your credit report at each of the three credit-reporting agencies.

43. If you are in the military and are deployed away from home, put an active duty alert on your credit report at each of the three credit-reporting agencies.

44. When using Wi-Fi, make sure that your wireless router has an encryption mechanism. Make sure that it is turned on.

45. Use complex passwords with combinations of letters and symbols, and use different passwords for each of your accounts.

46. File your income tax return early in order to avoid tax identity theft.

47. Never download tax software contained in an e-mail.

48. If you use a professional tax preparer, make sure that they are legitimate and that they protect your personal data.

49. If you e-file your income tax return, use a strong password and store the information on a CD or flash drive in a secure place rather than on your computer's hard drive.

50. If you file your income tax return by mail, do it from the post office and not a mailbox.

51. Opt out of information sharing when you receive notices from companies pursuant to the Gramm-Leach-Bliley Act.

52. Carefully evaluate your privacy settings on your social network sites, and set them up at a level with which you are comfortable.

53. Use the Do Not Track option for Internet Explorer and Mozilla Firefox 5 for your Internet browsing.

54. Set a security lockout on your smartphone when it is not in use.

55. Go to your social media only directly through its Web site.

56. It is nice to be friendly, but don't accept as a friend everyone who asks on Facebook or other social networks.

57. Check out the privacy policy of the various social networks you use.

58. Always investigate the legitimacy of an app before you install it.

Recap - Rules to Follow If You Are a Victim of Identity Theft

Cognizant of Murphy's Law that what can go wrong will go wrong, you might have followed all my rules for protecting yourself from becoming a victim of identity theft and still find yourself a victim because, as I explained earlier, your personal information may be in the data banks of companies and governmental agencies that might

not do a good job protecting your information. In that instance, here are some rules to follow:

1. Notify the credit-reporting agencies and have a fraud alert and a credit freeze placed on your account with each agency.

2. Report the crime to the appropriate law enforcement authorities where you live and where the fraud occurred. Use the FTC's ID Theft Affidavit.

3. Inform all your creditors that you have become a victim of identity theft.

4. Get new credit cards with new account numbers for all tainted accounts.

5. Set up passwords for new accounts.

6. Change your PINs.

7. When you close tainted accounts, make sure that the accounts are reported to the credit-reporting agencies as being closed at the customer's request due to identity theft.

8. Ask your creditors to notify each of the credit-reporting agencies to remove erroneous and fraudulent information from your file.

9. If your checks are stolen, promptly notify your bank and close the account immediately.

10. Notify the check-verification companies and request that they contact retailers that use their sendees to advise them not to accept checks from any checking accounts of yours that have been accessed by identity thieves.

11. Contact the creditors who have tainted accounts in your name and request that they initiate a fraud investigation. Get a copy of the completed investigation.

12. Send copies of those completed investigations to each of the credit-reporting agencies and request that erroneous and fraudulent information be removed from your files.

13. If fraudulent charges do manage to appear on your credit report, notify the credit-reporting agencies in writing and tell them that you dispute the information and request that such information be removed from your files.

14. If you are contacted by a debt collector attempting to collect on a debt incurred by an identity thief, inform the debt collector that the debt is not yours and that you are a victim of identity theft.

15. If your passport is lost or stolen, contact the State Department to report it lost or stolen and to get a new passport.

16. If you are a victim of criminal identity theft, contact the police and local District Attorney's office to clear your name. Get a letter from the District Attorney explaining that you have been a victim of criminal identity theft and carry it with you at all times.

17. Be aware of identity thieves who will take advantage of the information they have gained about you to contact you under the guise of assisting you in fixing your identity theft.