How to Keep Your Personal Information Secure

Protecting your personal information can help you reduce your risk of identity theft. There are four main ways to do it: know who you share information with; store and dispose of your personal information securely, especially your Social Security number; ask questions before deciding to share your personal information; and to maintain appropriate security on your computers and other electronic devices.

Keeping Your Personal Information Secure Offline

Lock your financial documents and records in a safe place at home, and lock your wallet or purse in a safe place at work. Keep your information secure from roommates or workers who come into your home.

Limit what you carry. When you go out, take only the identification, credit, and debit cards you need. Leave your Social Security card at home. Make a copy of your Medicare card and black out all but the last four digits on the copy. Carry the copy with you — unless you are going to use your card at the doctor's office.

Before you share information at your workplace, a business, your child's school, or a doctor's office, ask why they need it, how they will safeguard it, and the consequences of not sharing. Shred receipts, credit offers, credit applications, insurance forms, physician statements, checks, bank statements, expired charge cards, and similar documents when you don't need them any longer.

Destroy the labels on prescription bottles before you throw them out. Don't share your health plan information with anyone who offers free health services or products.

Take outgoing mail to post office collection boxes or the post office. Promptly remove mail that arrives in your mailbox. If you won't be home for several days, request a vacation hold on your mail.
When you order new checks, don't have them mailed to your home, unless you have a secure mailbox with a lock.

Consider opting out of prescreened offers of credit and insurance by mail. You can opt out for 5 years or permanently. To opt out, call 1-888-567-8688 or go to optoutprescreen.com. The 3 nationwide credit reporting companies operate the phone number and website. Prescreened offers can provide many benefits. If you opt out, you may miss out on some offers of credit.

Keeping Your Personal Information Secure Online

Know who you share your information with. Store and dispose of your personal information securely.

Be Alert to Impersonators

Make sure you know who is getting your personal or financial information. Don't give out personal information on the phone, through the mail or over the Internet unless you've initiated the contact or know who you're dealing with. If a company that claims to have an account with

you sends email asking for personal information, don't click on links in the email. Instead, type the company name into your web browser, go to their site, and contact them through customer service. Or, call the customer service number listed on your account statement. Ask whether the company really sent a request.

Safely Dispose of Personal Information

Before you dispose of a computer, get rid of all the personal information it stores. Use a wipe utility program to overwrite the entire hard drive.

Before you dispose of a mobile device, check your owner's manual, the service provider's website, or the device manufacturer's website for information on how to delete information permanently, and how to save or transfer information to a new device. Remove the memory or subscriber identity module (SIM) card from a mobile device. Remove the phone book, lists of calls made and received, voicemails, messages sent and received, organizer folders, web search history, and photos.

Encrypt Your Data

Keep your browser secure. To guard your online transactions, use encryption software that scrambles information you send over the internet. A "lock" icon on the status bar of your internet browser means your information will be safe when it's transmitted. Look for the lock before you send personal or financial information online.

Keep Passwords Private

Use strong passwords with your laptop, credit, bank, and other accounts. Be creative: think of a special phrase and use the first letter of each word as your password. Substitute numbers for some words or letters. For example, "I want to see the Pacific Ocean" could become 1W2CtPo.

Don't Overshare on Social Networking Sites

If you post too much information about yourself, an identity thief can find information about your life, use it to answer 'challenge' questions on your accounts, and get access to your money and personal information. Consider limiting access to your networking page to a small group of people. Never post your full name, Social Security number, address, phone number, or account numbers in publicly accessible sites.

Securing Your Social Security Number

Keep a close hold on your Social Security number and ask questions before deciding to share it. Ask if you can use a different kind of identification. If someone asks you to share your SSN or your child's, ask:

- why they need it
- how it will be used
- how they will protect it
- what happens if you don't share the number

The decision to share is yours. A business may not provide you with a service or benefit if you don't provide your number. Sometimes you will have to share your number. Your employer and financial institutions need your SSN for wage and tax reporting purposes. A business may ask for your SSN so they can check your credit when you apply for a loan, rent an apartment, or sign up for utility service.

Keeping Your Devices Secure

Use Security Software

Install anti-virus software, anti-spyware software, and a firewall. Set your preference to update these protections often. Protect against intrusions and infections that can compromise your computer files or passwords by installing security patches for your operating system and other software programs.

Avoid Phishing Emails

Don't open files, click on links, or download programs sent by strangers**.** Opening a file from someone you don't know could expose your system to a computer virus or spyware that captures your passwords or other information you type.

Be Wise About Wi-Fi

Before you send personal information over your laptop or smartphone on a public wireless network in a coffee shop, library, airport, hotel, or other public place, see if your information will be protected. If you use an encrypted website, it protects only the information you send to and from that site. If you use a secure wireless network, all the information you send on that network is protected.

Lock Up Your Laptop

Keep financial information on your laptop only when necessary. Don't use an automatic login feature that saves your user name and password, and always log off when you're finished. That way, if your laptop is stolen, it will be harder for a thief to get at your personal information.

Read Privacy Policies

Yes, they can be long and complex, but they tell you how the site maintains accuracy, access, security, and control of the personal information it collects; how it uses the information, and whether it provides information to third parties. If you don't see or understand a site's privacy policy, consider doing business elsewhere.

Identity Theft Protection Services

If you're concerned about data breaches or identity theft, you may be considering signing up for identity theft protection services. Before you enroll, it's important to weigh the costs and benefits of various types of services. You can also compare them with free and low-cost services. The government's identityTheft.gov website provides free personal recovery plans and step-by-step guidance to help identify theft victims recover.

What are identity theft protection services?

Many companies refer to their services as *identity theft protection services*. In fact, no service can protect you from having your personal information stolen. What these companies offer are monitoring and recovery services. *Monitoring services* watch for signs that an identity thief may be using your personal information. *Recovery services* help you deal with the effects of identity theft after it happens.

Monitoring and recovery services are often sold together, and may include options like regular access to your credit reports or credit scores.

Monitoring Services

There are two basic types of monitoring services — credit monitoring and identity monitoring. ***Credit monitoring*** tracks activity on your credit reports at one, two, or all three of the major credit reporting agencies (CRAs) — Equifax, Experian, and TransUnion. If you spot activity that might result from identity theft or a mistake, you can take steps to resolve the problem before it grows. Usually, credit monitoring will alert you when:

- a company checks your credit history
- a new loan or credit card account is opened in your name
- a creditor or debt collector says your payment is late
- public records show that you've filed for bankruptcy
- there is a legal judgment against you
- your credit limits change
- your personal information, like your name, address, or phone number, changes

Credit monitoring **only** warns you about activity that shows up on your credit report. But many types of identity theft won't appear. For example, credit monitoring won't tell you if an identity thief withdraws money from your bank account, or uses your Social Security number to file a tax return and collect your refund.

Some services only monitor your credit report at one of the CRAs. So, for example, if your service only monitors TransUnion, you won't be alerted to items that appear on your Equifax or Experian reports. Prices for credit monitoring vary widely, so it pays to shop around. Questions to ask credit monitoring service providers:

- Which credit reporting agencies do you monitor?
- How often do you monitor CRA reports? Some monitor daily; others are less frequent.

- What access will I have to my credit reports? Can I see my reports at all three CRAs? Is there a limit to how often I can see my reports? Will I be charged a separate fee each time I view a report?
- Are other services included, such as access to my credit score?

Identity monitoring alerts you when your personal information — like your bank account information or Social Security, driver's license, passport, or medical ID number — is being used in ways that generally don't show up on your credit report. For example, identity monitoring services may tell you when your information shows up in:

- change of address requests
- court or arrest records
- orders for new utility, cable, or wireless services
- payday loan applications
- check cashing requests
- social media
- websites that identity thieves use to trade stolen information

To find out if your information is being misused, identity monitoring services must check databases that collect different types of information to see if they contain new or inaccurate information about you. For example, they might check the National Change of Address database to see if anyone is trying to redirect your mail. The effectiveness of the monitoring will depend on factors like the kinds of databases the service checks, how good the databases are at collecting information, and how often the service checks each database. There also may be information that a service cannot monitor. For example, most monitoring services can't alert you to tax or government benefits fraud, including Medicare, Medicaid, welfare, and Social Security frauds.
Questions to ask identity monitoring providers:

- What kinds of information do you check, and how often? For example, does the service check databases that show payday loan applications to see if someone is misusing your information to get a loan?
- What personal information do you need from me and how will you use my information?
- Are other services included with the identity monitoring service? Do they cost extra?

Identity recovery services

Identity recovery services are designed to help you regain control of your good name and finances after identity theft occurs. Usually, trained counselors or case managers walk you through the process of addressing your identity theft problems. They may help you write letters to creditors and debt collectors, place a freeze on your credit report to prevent an identity thief from opening new accounts in your name, or guide you through documents you have to review. Some services will represent you in dealing with creditors or other institutions if you formally grant them authority to act on your behalf.

Identity theft insurance

Identity theft insurance is offered by most of the major identity theft protection services. The insurance generally covers only out-of-pocket expenses directly associated with reclaiming your identity. Typically, these expenses are limited to things like postage, copying, and notary costs. Less often, the expenses might include lost wages or legal fees. The insurance generally doesn't reimburse you for any stolen money or financial loss resulting from the theft.

As with any insurance policy, there may be a deductible, as well as limitations and exclusions. Also, most policies don't pay if your loss is otherwise covered by your homeowner's or renter's insurance. If you're interested in identity theft insurance, ask to see a copy of the company's terms and conditions.

Alternatives to commercial identity theft protection services

Here are some low-cost — or free — ways you can protect yourself against identity theft:

- Monitor your credit reports for free. Federal law requires each of the three major credit reporting agencies to give you a free credit report — at your request — each year. Visit AnnualCreditReport.com — the only authorized website for free credit reports. If you want to monitor your reports over time, you can spread out your requests, getting one free report every four months.
- Review statements for your credit card, bank, retirement, brokerage, and other accounts every month. Or log in and check them even more frequently. They can tip you to fraudulent charges on your accounts long before issues show up on your credit report.
- Review the explanation of benefits (EOB) statements you get from your health insurance providers. If you see treatments you never received, immediately tell your insurer and medical providers.
- Consider placing a credit freeze — also known as a security freeze — on your credit files with the major credit bureaus. A credit freeze blocks anyone from accessing your credit reports without your permission. Because potential creditors can't check your files, a credit freeze generally stops identity thieves from opening new accounts in your name.

To freeze your credit files, you'll have to contact each of the CRAs separately. If you opt for a freeze, each time you need to allow a company to check your credit — for example, if you apply for a loan or an apartment — you'll have to unlock your file. The process can take a few days. And, unless you already are an identity theft victim, there may be a fee each time you unfreeze and refreeze your credit. Fees vary based on where you live, but commonly range from $5 to $10.

If you want to both freeze your credit and get monitoring services, sign up for the monitoring service **before** placing the credit freeze. That way, the monitoring service can get access to your credit files. Otherwise, you may not be able to complete the service's account creation process. If you lift the freeze to give the service access, restore it as soon as possible.

- Consider taking advantage of free identity theft protection services that businesses and the government may offer you after a data breach. Check out any company online before enrolling. Some scammers send fake "free" offers to steal your personal information.
- If you believe you are an identity theft victim or are at risk of becoming one — possibly because you received a data breach notice or your wallet was lost or stolen — you can

place a free, initial 90-day fraud alert on your credit report. The alert tells potential creditors and lenders to contact you directly and verify your identity before opening new accounts in your name. You can renew the fraud alert after 90 days, or remove it at any time.

To place an initial alert, contact one of the three credit reporting agencies. The agency you contact must tell the other two agencies about your alert. You'll get a letter from each CRA confirming that it placed a fraud alert on your file. The letter also will tell you that you are entitled to a free credit report — even if you already ordered your free annual credit report this year — and explain how to request the report. You will have to separately request a free report from each CRA.

IdentityTheft.gov Offers Free Personal Recovery Plans

Visit IdentityTheft.gov if you believe you have been the victim of identity theft, or if your personal information has been lost or exposed. IdentityTheft.gov is the government's free, one-stop resource for reporting and recovering from identity theft. The website, available in Spanish at RobodeIdentidad.gov, will provide you with a personal, interactive recovery plan tailored to your individual identity theft needs. It will:

- Walk you through each recovery step
- Generate pre-filled letters, affidavits, and forms for you to send to credit bureaus, businesses, debt collectors, and the IRS
- Adapt to your changing needs, provide you with follow-up reminders, and help you track your progress
- Provide advice about what to do if you're affected by specific data breaches

IdentityTheft.gov has recovery plans for more than 30 types of identity theft, including tax-related identity theft and identity theft involving a child's information. Please check out this video to learn more about the website

For more information or similar articles as this one, visit the Federal Trade Commission's website at www.ftc.gov.