What To Know About Identity Theft

What Is Identity Theft? Identity theft is when someone uses your personal or financial information without your permission.

Taking steps to protect your personal information can help you avoid identity theft. Here's what you can do to stay ahead of identity thieves.

Keep your financial records, Social Security and Medicare cards, and any other documents that have personal information in a safe place. When you decide to get rid of those documents, shred them before you throw them away. If you don't have a shredder, look for a local shred day, or use a marker to block out account numbers. If you get statements with personal information in the mail, take your mail out of the mailbox as soon as you can.

Some organizations need your Social Security number to identify you. Those organizations include the IRS, your bank, and your employer. Organizations like these that do need your Social Security number won't call, email, or text you to ask for it.
Other organizations that might ask you for your Social Security number might not really need it. Those organizations include a medical provider, a company, or your child's school. Ask these questions before you give them your Social Security number: 1) Why do you need it? 2) How will you protect it? 3) Can you use a different identifier? And 4) Can you use just the last four digits of my Social Security number?

If you're logging in to an online account, use a strong password. Add multi-factor authentication for accounts that offer it. Multi-factor authentication offers extra security by requiring two or more credentials to log in to your account. The additional credentials you need to log in to your account fall into two categories: something you have — like a passcode you get via text message or an authentication app, or something you are — like a scan of your fingerprint, your retina, or your face. Multi-factor authentication makes it harder for scammers to log in to your accounts if they do get your username and password. Do not give your personal information to someone who calls, emails, or texts you. It could be a scammer trying to steal your information.

In addition to taking steps to protect your information, **it pays to know how to tell if someone stole your identity**. There are things you can do yourself to detect identity theft. There also are companies that sell credit and identity monitoring services.

Here's what you can do to spot identity theft:

- **Track what bills you owe and when they're due.** If you stop getting a bill, that could be a sign that someone changed your billing address.
- **Review your bills.** Charges for things you didn't buy could be a sign of identity theft. So could a new bill you didn't expect.
- **Check your bank account statement.** Withdrawals you didn't make could be a sign of identity theft.

- **Get and review your credit reports.** Accounts in your name that you don't recognize could be a sign of identity theft. Here's how you can get your free credit reports.

Many companies sell identity theft protection services that may include credit monitoring, identity monitoring, identity recovery services, and identity theft insurance. These services also might be offered by your

- bank or credit union
- credit card provider
- employer's benefits program
- insurance company

Credit monitoring services scan activity that shows up on your credit reports. They might monitor activity at one, two, or all three of the major credit bureaus — Equifax, Experian, and TransUnion.

Credit monitoring services will usually alert you when: a company checks your credit history; a new loan or credit card account appears on your credit reports; a creditor or debt collector says your payment is late; public records show that you filed for bankruptcy; someone files a lawsuit against you; your credit limit changes; and your personal information, like your name, address, or phone number, changes.

Credit monitoring services **will not** alert you when someone withdraws money from your bank account; or when someone uses your Social Security number to file a tax return and collect your refund.

Companies that offer identity monitoring services check databases that collect different types of information to see if they contain new or inaccurate information about you. Those could be a sign that someone is using your personal information. These services can detect uses of your personal information that won't show up on your credit report.

Companies that sell credit and identity monitoring services also may offer identity recovery services to help you fix any damage caused by identity theft. These services may be included or cost extra. Some of the services they offer may be things you can do on your own for little or no cost. Identity recovery services typically give you access to counselors or case managers who will help you recover your identity. 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; and guide you through documents you have to review.

Identity theft insurance generally won't reimburse you for money stolen or financial loss resulting from the theft. Most policies won't pay if your loss is covered by your homeowner's or renter's insurance. If you're considering getting identity theft insurance, ask about the deductible and find out what's covered and what isn't. For more information, visit: https://www.consumer.ftc.gov/articles/what-know-about-identity-theft

If you have further questions, please email us at: USARMY.WIESBADEN.USAREUR.MBX.OJA-WLC-LEGAL-ASSISTANCE-CALENDAR@ARMY.MIL.