IDENTITY THEFT PROTECTION BEGINS WITH YOU!

IDENTITY THEFT CANNOT BE TOTALLY PREVENTED.

Your personal information is most likely already in one or dozens of third party data bases such as airlines, rental car companies, credit card companies, banks, insurance companies, medical records, retail merchants, associations and more. Data breaches now occur nearly weekly in the US alone.

First Step:

Purchase individual or family identity theft protection. Identity theft protection will provide resolution services in the event your or your family member's identity stolen and used for fraudulent purposes. Without it, you could spend a lifetime trying to restore your credit and good name, and pay a fortune in legal fees.

Second Step:

Education is the key to helping you protect yourself against identity theft. Learn what identity theft is and how you can take daily measures to protect yourself and your family.

What is Identity Theft?

Identity theft is a crime where a thief steals your personal information, such as your full name, Date of Birth, Driver License, and or Social Security number, to commit fraud. The identity thief can use your personal information to fraudulently apply for credit, file taxes, or get medical services. These acts can damage your credit status, and cost you time and money to restore your good name. You may not know that you are the victim of ID theft until you experience a financial consequence (mystery bills, credit collections, and denied loans) down the road, from actions that the thief has taken with your stolen identity.

There are common types of identity theft that can affect you:

- **Cyber ID theft** – Many personal computers are vulnerable to viruses and malware that can hack into your email address book and also extract personal information from files you may store on your computer. Spam emails can entice you to provide personal information to the criminal on the other end, or get you to download viruses and malware.
- **Child ID theft** - Children's IDs are vulnerable because the theft may go undetected for many years. By the time they are adults, the damage has already been done to their identities.

- **Tax ID theft** - A thief uses your Social Security number to falsely file tax returns with the Internal Revenue Service or state government.
- **Medical ID theft** - This form of ID theft happens when someone steals your personal information, such as your Medicare ID or health insurance member number to get medical services, or to issue fraudulent billing to your health insurance provider.
- **Senior ID theft** - ID theft schemes that target seniors. Seniors are vulnerable to ID theft because they are in more frequent contact with medical professionals who get their medical insurance information, or caregivers and staff at long-term care facilities that have access to personal information or financial documents.
- **Social ID theft** - A thief uses your name, photos, and other personal information to create a phony account on a social media platform.

Sites to Visit:

While you cannot completely prevent ID theft from occurring, there are ways to protect yourself. Taking proactive steps now can reduce the debilitating impacts of the crime and help you restore your good name more quickly. Education is the key. Safeguard yourself against this crime today. Visit one or more of the sites below for additional information on identity theft and identity theft protection.

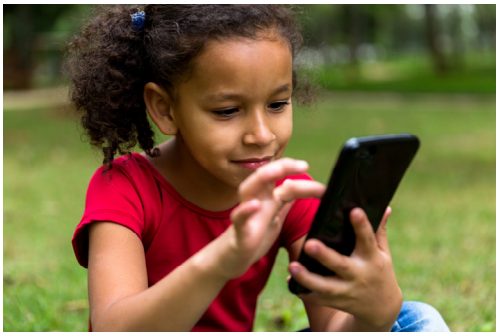
www.usa.gov/identity-theft#item-206114
www.ftc.gov
www.privacyrights.org
www.idtheftcenter.org

Prevention Tips

1. Secure your Social Security number (SSN). Don't carry your Social Security card in your wallet or write your number on your checks. Only give out your SSN when absolutely necessary.
2. Don't respond to unsolicited requests for personal information (your name, birthdate, Social Security number, or bank account number) by phone, mail, or online.
3. Contact the three credit reporting agencies to request a freeze of your credit reports.
4. Collect mail promptly. Place a hold on your mail when you are away from home for several days.

5. Pay attention to your billing cycles. If bills or financial statements are late, contact the sender.
6. Enable the security features on mobile devices, especially if you have contacts, banking websites and applications saved.
7. Update sharing and firewall settings when you're on a public Wi-Fi network. Consider using a virtual private network, which can give you the privacy of secured private network. You can even use the “Dark Web” browser and an anonymous email address to discourage “hacking” into your computer.
8. Review your credit card and bank account statements regularly. Promptly compare receipts with account statements. Watch for unauthorized transactions.
9. Shred receipts, credit offers, account statements, and expired credit cards, to prevent “dumpster divers” from getting your personal information.
10. Store personal information in a safe place.
11. Install firewalls and virus-detection software on your home computer.
12. Create complex passwords that identity thieves cannot guess easily. Change your passwords if a company that you do business with has a breach of its databases
13. Review your credit report once a year to be certain that it doesn't include accounts that you have not opened. You can order it for free from Annualcreditreport.com.

Identity Thieves Stealing Children’s Identities



A new study from Javelin Strategy & Research shows that one million U.S. children fell victim to identity fraud in 2017.

Financial losses stemming from those fraud incidents against children were significant. According to Javelin, total losses amounted to $2.6 billion and more than $540 million in "out-of-pocket" costs linked to child-identity theft were lost.

"Child-identity fraud is a serious problem and is frequently overlooked as the public focuses on high-profile breaches involving the personally identifiable information of adults," says Al Pascual, head of fraud and security at Javelin Strategy & Research. "Child-

identity fraud has unique characteristics that make it particularly hard to prevent, though there are steps parents and guardians can take to help keep children safe."

For parents, the route to safety starts with education, some old-fashioned due diligence, along with a handful of useful data security technology tools, experts say.

Get your kids up to speed early on identity-fraud risks. "Start training children to protect their identity in the digital world when they are young," Javelin sates. "Early training for children to properly manage their online activity will instill habits invaluable in their adulthood, reducing their risk of victimization early and later in life."

Your Defense

1. Watch for signs your child is being bullied. There is a "strong relationship" between fraud and bullying.

2. Order a credit report from Equifax on your child's behalf.

3. Implement a credit freeze where possible (some states do not allow on minors).

4. Look out for red flags like unexpected bills, collections, or IRS contacts that reference their child's name as well as a lot of pre-approved credit offers'.

5. Protect your child's Social Security number at all cost.