

Identity Theft Protection Tips

Data breaches of personally identifiable information have unfortunately become more common these days and can lead to identity theft. While organizations do their best to protect against cybersecurity attacks and data leaks, what can you do to protect yourself?

Help Protect Yourself

1. Enroll in an identity theft monitoring service:

Credit monitoring and identity theft monitoring are often combined now. You can do this either by purchasing a service offered by many companies, or if your data is involved in a large data breach, credit monitoring may be offered to you for free for some period of time. Some individuals express concern about entering all of their personal information into yet another service and risk getting it stolen. While nothing is zero risk, the risk of not doing so is much larger than the risk of using it.

Example services (not an endorsement):

- <https://www.experian.com/consumer-products/identity-theft-and-credit-protection.html>
- <https://www.idx.us/idx-identity>
- <https://www.identityguard.com/>
- <https://www.privacyguard.com/>
- <https://www.lifelock.com/>
- <https://www.costco.com/identity-protection-services.html>

2. Freeze your credit:

Strongly consider freezing your credit reports with all three agencies, or at least enabling fraud alerts. This prevents criminals from opening lines of credit in your name and ruining your credit score. You can easily “unfreeze” your credit report temporarily whenever you legitimately need it accessed in the future.

- <https://consumer.ftc.gov/articles/what-know-about-credit-freezes-fraud-alerts>
- <https://oag.ca.gov/idtheft/facts/freeze-your-credit>
- <https://www.nerdwallet.com/article/finance/how-to-freeze-credit>
- <https://www.equifax.com/personal/credit-report-services/>
- <https://www.experian.com/freeze/center.html>
- <https://www.transunion.com/credit-freeze>

IDENTITY THEFT PROTECTION TIPS



3. File your tax returns quickly each tax season

Filing as soon as possible prevents criminals from filing fraudulent tax returns in your name and getting a check mailed to them instead of you, as they will file for a refund, not pay your bill. You can also get an Identity Protection PIN from the IRS so that nobody else can file a return in your name without also using that special PIN.

4. Register your online accounts with government agencies

Ensure that you've registered for an online account with important government agencies using your identity before an unauthorized person does.

- <https://www.ssa.gov>
- <https://www.irs.gov/payments/view-your-tax-account>
- <https://www.ftb.ca.gov/myftb/index.asp>
- https://edd.ca.gov/Benefit_Programs_Online.htm
- <https://informeddelivery.usps.com>

5. Monitor your financial statements

Review your bank account statements more closely for suspicious transactions and enable fraud alerts if your bank supports them, immediately report anything suspicious to your financial institution.

6. Be mindful of your passwords and account reset questions

Don't use passwords or account recovery secret questions/answers that can be inferred from your personal information. Consider using randomly generated input unique to each online account instead and store answers in a secure password manager, such as 1password. Also enable multi-factor authentication on all online accounts that support it.

7. Watch out for threatening emails or phone calls

Watch out for suspicious emails or social engineering attempts to threaten you into giving criminals money. Do not respond to them or click any links, and forward it to securinginfo@sdcoe.net