5 Low Cost Ways to Protect Against Identity Theft

By Eileen Ambrose, Kiplinger.com, 6/12/25

Stay ahead of identity thieves and maintain your peace of mind with these simple, affordable steps.

You're careful about sharing your information to protect yourself against identity theft, but not everyone who has your personal data may be as vigilant as you.

For example, in the past year, eight out of 10 consumers received a data breach notice, alerting them that their private information may have been compromised, according to a 2024 report by the Identity Theft Resource Center.

With some key information about you, a thief can open credit card accounts, receive medical care under your name, or file a bogus tax return and claim a refund. It could take months to recover, depending on the type of ID fraud. Identity theft involving a tax return can take nearly two years to resolve, during which time the victim's refund is delayed, says the National Taxpayer Advocate.

But taking a few preventative measures that cost little or no money can help thwart thieves. You can, for instance, restrict who gets access to your credit report information, making it harder for criminals to open accounts in your name. Or, you can enroll in an identity theft protection service, such as LifeLock, that alerts you to suspicious bank or credit card activity and helps restore your identity if you become a victim.

Here are five simple and affordable steps to protect your identity and finances:

1. Learn the signs of ID theft.

The earlier you recognize suspicious activity in your accounts, the quicker you can stop thieves or limit the damage they can do.

Here are several signs that you may be a victim of ID theft:

- An unexpected, sudden, and steep drop in your credit score.
- Unauthorized withdrawals from your bank account.
- Bills for medical care you didn't receive.
- You no longer receive bills or any other mail, indicating a criminal might have switched your mailing address.
- Calls from debt collectors about outstanding bills that don't belong to you.
- You see charges on your credit card statement that you don't recognize. (Be aware, a legitimate charge may appear under a different name used by the merchant. So double-check the purchase.)
- You receive a rejection for credit you didn't apply for.
-

2. Create unique passwords.

These should be at least 12 characters, including uppercase and lowercase letters, numbers, and symbols. Avoid the obvious, such as "123456," "qwerty," and "password," or information that can be gleaned from your social media posts, such as your birthday or pet's name.

Each account should have a unique password. That way, if thieves learn one of your passwords, they won't be able to access all your accounts.

For an extra layer of protection, set up two-factor authentication on your accounts. With this, after you log in with your password, you will be asked to type in a second factor, such as a code sent to you via email or text.

It's not unusual for someone to have dozens of accounts needing passwords. If you're among those with more passwords than you can easily remember, consider using a password manager that can generate and safely store unique passwords for each of your accounts. All you have to do is remember one master

password to access your accounts. Some password managers charge an annual fee, but free versions, such as Norton Password Manager, are available.

3. Monitor your accounts and credit reports.

Review your financial statements for any suspicious activity. And if you spot a problem, report it to the bank or creditor immediately to limit the damage.
Credit card issuers generally have a "zero liability" policy, meaning you won't be charged for fraudulent purchases.
But with debit cards, your liability will be determined by when you reported the fraud. For example, if you notify your bank within two days of discovering that your debit card was lost or stolen, your liability is capped at $50 for unauthorized transactions. Wait longer than two days but less than 60 days after getting your bank statement, and you could be liable for up to $500. Delay longer, and you could be out the full amount stolen by a criminal.
To help you detect fraud early, you can set up alerts from your bank. You can, for instance, request text or email alerts when a credit or debit card transaction exceeds a certain limit or your card is used outside the U.S.
Also, periodically review your credit reports for errors or unusual activity. You can receive free copies of your credit report each week from the major credit reporting companies — Equifax, Experian, and TransUnion — through AnnualCreditReport.com.

4. Freeze out thieves.

At no cost, you can place a security "freeze" on your credit reports, which will prevent any new creditor from seeing them. Without being able to view your reports, a creditor is unlikely to open any new line of credit under your name. You can also temporarily lift the freeze when you need to apply for credit.

To freeze your reports, you can contact each credit reporting company by phone, mail, or online.

5. Consider identity theft protection.

Staying ahead of thieves requires vigilance, which can take a lot of time and effort. That's where an identity theft protection service can provide peace of mind by helping you deal with identity theft if it happens.

For example, LifeLock, a leader in identity theft protection in the U.S., offers a variety of plans with different levels of protection and prices to fit your needs and budget.

Identity theft isn't going away. In 2024 alone, the Federal Trade Commission received 1.1 million stolen-identity complaints from consumers. By using these five simple steps, though, you may be able to avoid joining them.