Personal Finance

Should You Pay for Identity Theft Protection?

Monitoring services can help you spot red flags quickly, but they won't stop criminals from targeting you.

(Image credit: Getty Images)

"An ounce of prevention is worth a pound of cure." When Benjamin Franklin penned this enduring phrase nearly three centuries ago, he was advising the public on how to avoid house fires. But his words are also useful when applied to a modern safety issue: identity theft.

By some estimates, roughly one-third of U.S. residents have experienced some form of identity theft—a crime that includes everything from credit card theft to tax fraud to insurance fraud—and that figure is expected to rise. For some consumers, the instinct is to turn to a familiar brand such as Norton, Equifax or McAfee for protection. Each of them offers something different, and you can subscribe to one of their plans for yourself or your family for just a few dollars a month (or in some cases, for free).

Do ID theft protection services really work?

It depends on what you're looking for. Identity theft plans typically include some combination of account monitoring, alerts and restoration support. In other words, they don't stop criminals from targeting you—they just respond

to identity theft once it has happened.

“ID protection services largely entail cleanup rather than prevention,” says Mitch Mayne, a cybersecurity consultant and former incident responder for IBM Security X-Force. “While these services can offer some benefits to victims, they also create a false sense of security, which leads users to neglect basic cyber hygiene.”

According to Aura, a company that provides identity theft protection plans, you don’t necessarily need ID protection services. “While monitoring and fraud alerts are valuable ways to protect your identity, they don’t do anything you can’t do on your own,” Aura’s website says.

If you do decide to pay for ID protection, keep in mind that not all plans are created equal. The best plans come with tried-and-true, unfussy features such as VPNs, which hide your IP address and encrypt your data while you browse the internet, and password managers, which generate and store unique passwords for each of your accounts. A password manager may be the most valuable offering. “Sign-in credentials are frequently compromised and quickly sold on the dark web,” says Mayne, “so a password manager can provide some solid risk mitigation.”

Many plans, however, are packed with flashy features that may not deliver, such as identity theft insurance, which typically covers the costs you incur during the recovery process but doesn’t cover your financial losses, and live restoration support, which gives you access to live customer service agents after you experience an identity theft incident or receive an alert that your information may have been compromised. “It can be incredibly difficult to get an insurance claim approved by an ID theft monitoring company,” Mayne warns, “and even with their help responding to an incident, it can take years to get your money back and restore your identity. For some people, the damage is never fully undone.”

A multipronged approach

These services are not a cure-all for the myriad threats your identity faces, but when combined with good habits (more on those below), some targeted services can help.

For example, DeleteMe (https://joindeleteme.com), which has plans starting at $8.71 a month, helps prevent damage by finding and removing your personally identifiable information (PII) from data-broker websites. “Most of us have our PII available for purchase from multiple data-broker sites, so this removal lowers your risk footprint overall,” says Mayne.

For password management, 1Password (https://1password.com) is well-reviewed and highly recommended for its long list of security features, which include a mix of advanced encryption, biometrics (face and fingerprint identification) and ease of use. Plans start at $2.99 a month, and you can sign up for a free 14-day trial.

For more-comprehensive monitoring, prioritize services that offer restorative and preventative support. For example, both of the identity theft protection plans from IDShield (www.idshield.com) come with guaranteed identity restoration, which gives you unlimited access to live customer support, but they also include password managers and VPNs. They offer some degree of credit-score and credit-report monitoring as well. ID Shield plans start at $14.95 a month.

Consider the free alternatives

Many people don’t realize they already have free services available to them through their relationships with financial institutions. If you have a Mastercard credit card or debit card, for example, you can visit https://mastercardus.idprotectiononline.com to sign up for free restoration and monitoring services, including alerts if your user credentials are compromised in a corporate data breach. (Keep in mind that you have liability protections for your bank and credit card accounts, too. For example, American Express, Discover, Mastercard and Visa credit cards all come with zero-liability protection, which means you won’t have to pay a single dollar lost due to a fraudulent charge made on your account.) You may also have a free identity theft protection plan through your employer, and some renters and homeowners insurance policies include protection for financial accounts, too.

“Many identity theft protections already come with products you use—your antivirus software, for example,” says Mayne, “so it’s worth your time and money to understand what you already have available before buying another product that does the same thing.”

You can also explore free services online. For example, to find out if your information has been “pwned,” or compromised in a data breach, and sign up for future data breach alerts, try using Have I Been Pwned (https://haveibeenpwned.com). As for securing your credit reports and preventing certain forms of credit card fraud, you can set up a credit freeze, which blocks anyone from opening up a new loan or credit card in your name, by contacting the three national credit bureaus (Experian, Equifax and TransUnion). You can also visit AnnualCreditReport.com to pull your credit reports for free once a week and review them for signs of fraud, such as hard inquiries for loans and credit cards you have not applied for.

Perhaps the best news for people hoping to save money is that you are your own strongest defense against identity theft. “The best way to protect your identity is by consistently taking free, preventative actions,” says Mayne. That includes using unique and complex passwords for each of your accounts, enabling multifactor authentication for account sign-in, and installing software updates for your devices, apps and web browsers as soon as they’re available. Additionally, you should never click links or attachments that appear in unsolicited text messages and e-mails; they may lead to scam websites or install malware on your device.

Kiplinger