5 Easy Ways To
Protect Your Privacy

Allen St. John, Consumer Reports
January 2018

Update Your Devices

One of the easiest and most effective ways to protect the security of your computers and mobile devices is to keep the software up to date

Updates help manufacturers patch security vulnerabilities quickly.
For example, early this year Apple, Microsoft, and others released fixes for the Meltdown and Spectre security flaws that affected millions of laptops and other devices.

Every month there are updates for you PC, your Mac, your phones.
Make sure you apply them.

Use Two-Factor Authentication

What if you could find a way to make your password all but useless to a hacker?
That's what two-factor authentication does.

Instead of relying solely on a password, user accounts secured by two-factor authentication require an additional level of proof of ID before granting access.

This may involve the use of a physical device (like your phone, a card, or a fob) or some biometric marker (like a fingerprint, a voice print, or facial recognition).

How Two-Factor Authentication Typically Works

When you log in to an account on a new laptop or smartphone, you'll be asked for your password, but once you enter it, you won’t have access to your account.

Instead, the website will ask for a one-time code sent by text to your phone.
The second "factor" is your phone; without it and the password, you'll be denied access.

To find out how to enable it, just search for “two-factor authentication” online with the company name, such as Amazon, Apple, Gmail, or the name of your bank.

Freeze Your Credit

There's not much you can do to stop the next data breach, but you can minimize the financial risk with a credit freeze. That prevents most lenders from looking at your credit history, which keeps them from issuing a credit card or approving a loan to an unauthorized party.

The main problem is that a freeze also locks out vendors you are doing business with. That might include a mortgage lender or a carmaker's finance company and others like a cell-phone company or even a potential employer.

You need to initiate a freeze with each of the four major credit services: Experian, Equifax, TransUnion, and the lesser-known Innovis. And when you do file an application that requires a credit check, **you'll have to contact them individually to lift the freeze.**

As of 9/21/18 there is no charge to place or lift a credit freeze.

Where to go to put a security freeze on your account

Equifax: https://www.equifax.com/personal/credit-report-services/

Experian: https://www.experian.com/freeze/center.html

Transunion: https://www.transunion.com/credit-freeze

Innovis: https://www.innovis.com, Click on Security Freeze,
Click on "Submit Security Freeze Request online".
Fill out form and submit

Install a Password Manager

A password manager creates and then stores complicated, hard-to-hack passwords for all your online accounts, letting you access them with one simple-to-remember password.

Dashlane, 1Password, KeePass, and LastPass are among the most popular password managers.
They are either free or inexpensive ($2 to $5 a month).

While password managers are superb at helping you generate an effective new password and remember it, they can’t automatically replace all your existing passwords.

To lock down all your accounts, you have to log in to each one individually, opt to change your password, and then let your password manager do the rest.

To make it easier, focus on your most important accounts— your e-mail, bank, and healthcare accounts—and change the rest whenever you log in to them. Eventually all your accounts should be secured with new, stronger passwords locked away in your password manager.

Make Privacy a Priority

There's a lot to be said for choosing strong privacy protections whenever you sign up with a fresh online service or set up a new device.

Some of these settings can protect you from hackers. But they can also slow the erosion of your digital privacy that happens when tech companies collect and share information.

Retailers and social media companies rely on consumers to volunteer information. But just because they ask doesn't mean you have to answer.

As one example, look in your smartphone settings at what permissions each mobile app is asking for. Does it want access to the phone's microphone? Location data? Your contacts? If you're not sure why an app needs that information to function, turn off the permission. If that keeps the app from working the way you want, you can always switch it back on later.