SURVEILLANCE SELF-DEFENSE

A GUIDE FROM THE ELECTRONIC FRONTIER FOUNDATION

ENCRYPTION BEGINS AT HOME

The latest version of Windows, macOS, iOS and Android all have a way to encrypt your local files. Turn it on. Without it, anyone with a few minutes of physical access to your computer, tablet or smartphone can copy its contents, even if they don't have your password.
See https://eff.org/keeping-data-safe

END-TO-END ALL THE WAY

End-to-end encryption means that when you send a message, it's protected in a way that only the person you sent it to can read it. Neither your ISP, governments, nor others on your coffee shop's Wi-Fi will be able to take a peek. The easiest way to use end-to-end encryption is to download and install applications that support it: for instance, the messaging service Signal works on phones, laptops and desktop PCs. Note, however, that anyone with physical access to your unlocked phone will be able to see your in-app messages in plain text. So if your communications are highly sensitive, you may want to set the messages to disappear after you read them, so that they're removed from your device entirely. This is an option available in Signal.
See https://eff.org/end-to-end-all-the-way

ENCRYPT ALL THE (OTHER) THINGS

Even if you can't do end-to-end encryption, you can still encrypt a lot of your Internet traffic. If you use EFF's HTTPS Everywhere browser add-on for Chrome or Firefox, you can maximize the amount of web data you protect by forcing websites to encrypt webpages whenever possible. Use a virtual private network (VPN) when you're on a network you don't trust.
See https://eff.org/https-everywhere

FACTOR IN TWO-FACTOR

Two-factor authentication, where you type a password and a regularly changed confirmation number, helps protect you from password-stealing attacks when logging in to web and cloud services. Google has it; Facebook has it; even banks have it. When available, turn it on for the services you use. If it's not available, tell the service provider you want it.
See https://eff.org/2fa

STRONG PASSWORDS

Passwords these days have to be long to be safe against password-cracking techniques. Plus you need different passwords for every account you use. The strongest passwords are actually long passphrases—strings of random but memorable words. Check out EFF's diceware creator, which helps you create strong passphrases. You should also use a password manager, like 1Password, KeePassX, or LastPass. They keep all your passwords in one safe, encrypted place; allow you to remember just one master password; and can also help you generate strong passwords.
See https://eff.org/strong-passwords

LET GO OF ALL ATTACHMENTS

The easiest way to get intrusive malware onto your computer is through your email or compromised websites. Browsers are getting better at protecting you from the worst of the web, but files sent by email or downloaded from websites can still take complete control of your computer. Don't automatically click on attachments that claim to be Word documents, or any other files. Get your friends to send you information in the main body of the email instead; when you get a file (even from a friend), double-check it's really from them by calling or texting them first.
See https://eff.org/protect-against-malware

BE AN ALLY

We need your help. Urge your colleagues, friends and family to install secure software. Ask them to sign up for EFF updates, or join as a new member! Together, we can stop online spying and other malicious activity.

LEARN MORE: SSD.EFF.ORG