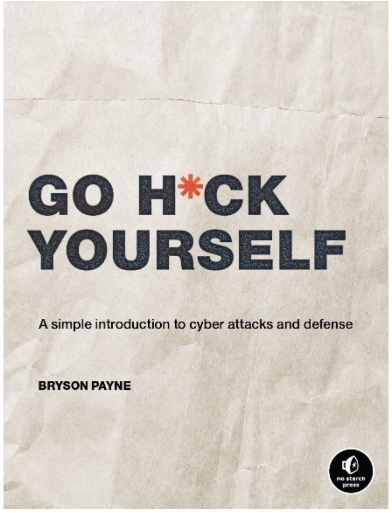
Hacking Yourself: Think Like a Hacker to Prevent Cyber Attacks

Ten things you can do right now to protect yourself online

Excerpt from *Go H*ck Yourself* (2022, No Starch Press) by Bryson Payne



❶ **Realize you're a target.** People say, "It'll never happen to me"— but a few smart precautions can help you avoid being an easy target for attackers. Knowing that you're a potential target is an important first step in protecting yourself and the people you care about.

❷ **Watch out for social engineering.** If someone is trying to get you to do something, either online or in person, stop and think about whether it's in your best interest. Block unwanted contacts, delete suspicious emails, hang up on robo-calls, and delete spam SMS text messages. (While you're at it, hold yourself back from sharing too much information on social media.)

❸ **Turn off devices and keep them physically secure.** Turn off Bluetooth and Wi-Fi when you're not using them. Close mobile apps when you're done with them. Turn off your computer and phone overnight if you can. Lock your doors, keep your devices with you, and be careful what you plug into your computer. If you walk away from your laptop for even a few minutes, an attacker can access your files or steal the computer.

❹ **Think before you click.** If you're unsure about the source of an email, don't open any links or attachments. Enter web sites in your browser rather than clicking through an email. Don't download illegal files or pirated software, music, or movies. Malicious hackers love to hide evil surprises in these "free" files. If a mobile app asks for too many permissions, delete it and find one that does what you want with fewer permissions.

❺ **Use a password manager and two-factor authentication.** Most people's passwords can be cracked in seconds. You only need to remember two passphrases of four or five words—one for your email and one for your password manager—and you can still have unique, almost uncrackable passwords for every account. For added protection, turn on two-factor authentication for your most important accounts.

❻ **Update your software regularly.** Turn on automatic updates for your operating system and update your browser and other apps at least monthly. Pick a certain day of the month, like the 1st or 30th, and mark your calendar to update your desktop, laptop, phone and all applications. Keeping your software up-to-date will eliminate over 99% of known attacks on the internet.

❼ **Protect your most sensitive data.** Don't log in to sensitive accounts on a public computer or an untrusted network. Instead, do sensitive work only on your most protected computer. Use a complex password and secure Wi-Fi at home, and check your router for unknown devices regularly, at least once a month. Consider encrypting your most sensitive files with BitLocker (PC), FileVault (Mac), or free, open-source VeraCrypt.

❽ **Turn on your firewall, antivirus, and VPN.** Keep your firewall turned on, and update your antivirus software weekly or turn on automatic updates. Firewalls and antivirus software can only protect you if they're turned on and up to date. Consider using a VPN app to protect your phone or laptop while traveling or using public Wi-Fi.

❾ **Back up the data you want to keep.** The best defense against losing data from ransomware, theft, destruction, or accidental deletion, is to back it up often. Back up your files to an external hard drive weekly or monthly, or use a cloud backup service for a few dollars a month. Search online for one that's highly rated and has the features you want and need.

❿ **Talk with your family.** Communicate, communicate, communicate. Set appropriate limits on your kids' screen time (based on their age), talk about online and real-world threats with younger and older relatives/friends, and listen to your kids – encourage them to talk to you if they're ever unsure what to do, or if they ever experience cyberbullying or harassment.