10 insider tricks to keep hackers and scammers from stealing from you

By Kim Komando, Komando.com, June 16, 2018

Cybercriminals are out in full force looking for ways to steal your data. It's worth money to them. That's why we've seen a massive uptick in the number of data breaches over the past few years.

Unfortunately, most folks don't know they've been hacked until it's too late. So you don't fall into that category, do one thing right now. Click here to see if your email address has been hacked or stolen.

With cybercrime so rampant, you need to be proactive about protecting yourself. To help you out, here are some things I do to keep hackers and scammers at bay.

1. Keep everything updated

First and foremost, it's vital to install updates as soon as you can, especially if they fix security bugs. Keep all your apps, smart appliances, and gadgets updated with the latest patches and firmware too.

The FBI recently issued a warning to anyone who owns a router. You need to reboot it. You can reboot it by unplugging it and then plug it back in after 30 seconds.

If hackers can find a flaw in a program or operating system, they can actively use it to attack computers until it gets patched.

2. Secure your devices already

Surprisingly, at least one-third of smartphone users don't bother to use even the simplest four-digit passcode to secure their gadgets. There are many ways to lock and unlock our phones, computers, and tablets -- face scans, thumbprints, irises, passcodes, patterns, and more.

Just set it up. It's a minor inconvenience that can save you a huge headache later.

3. Make sure your firewall is working

Even if hackers manage to know your computer's location and IP address, the firewall keeps them from accessing your system and your network. Not sure if you have a firewall in place? Newer Windows and Mac systems have built-in software firewalls for configuring your outgoing and incoming internet ports.

Wonder if your firewall is actually working? Click here for a free test.

4. Encrypt your drive

An extra layer of security you can employ is disk encryption. With encryption, your data will be converted into unreadable code that can only be deciphered with a specific key or password.

PC users can enable Windows' built-in encryption tool BitLocker. BitLocker is available to anyone with a machine running Windows Vista or 7 Ultimate, Windows Vista or 7 Enterprise, Windows 8.1 Pro, Windows 8.1 Enterprise, or Windows 10 Pro. It is not available on Windows 10 Home

Macs have their own built-in disk encrypting tool too called FileVault. Similar to BitLocker, it helps prevent unauthorized access to your data and adds an extra layer of security in case your computer is stolen or lost.

5. Don't trust public Wi-Fi

Crooks use public Wi-Fi to spy on unsuspecting users who join the network. Or, sometimes they even create "honeypot" networks, which are fake networks designed to steal your information.

If you're not careful, cybercriminals at your local cafe can walk away with your name, address, Social Security number, email address, and your usernames and passwords.

This is why it's critical that you use a virtual private network (VPN) when in public. It's a good idea to use one at home, too. With a VPN, your gadget's IP address is hidden from websites and services that you visit, and you're able to browse anonymously. Note from Tom: You can use an ethernet cable to connect your laptop or desktop to your router. That is safer (no wifi) and a little bit faster.

6. Completely wipe old devices that you're getting rid of

Just like a real trash can, the contents of your PC's Recycle Bin or Mac's Trash Can are only cleared out when you empty them. Using the same analogy, if it's been a while since you've emptied them, there's a treasure trove of documents and items for someone to snoop through.

If you want to get serious about your security, you need to erase sensitive data for good. Use software tools like Eraser or Blank and Secure for Windows and Secure Delete - File Shredder for Macs.

Favorite cross-platform tool free CCleaner for PCs and Macs also has an option for secure deletion of files.

7. Remember strong, unique passwords

Your password is the first line of defense. You want to make sure you set up a secure, unique password for every account. If you're feeling overwhelmed with passwords or want to develop harder passwords, consider using a password manager. A password manager (e.g. LastPass) is a program that can store and manage your passwords for each app, service, and site that you use. It's like a locked safe (or a vault) for all your credentials, tightly secured with your key.

8. Use two-factor authentication

Two-factor identification is a fancy name for adding an extra verification step to the login process of your most critical accounts. Instead of just providing your username or password to log in to an account, a secondary form of verification is required to prove your identity.

The most popular form of 2FA right now is a unique one-time code that's texted to your smartphone.

9. Use the guest network option

Friends and family always want to use your Wi-Fi. They ask politely, phone in hand because they hate to burn up their data plans when they can use your connection. Instead of handing them your real password, use your router's "Guest Network."

This feature lets you share your internet connection with your guests while keeping them off your primary network, preventing them from seeing your shared files and services. To avoid confusion with your primary network, set up your guest network with a different network name (SSID) and password.

10. Pick the right account type

When you first set up a computer, you create at least one user account. If you have several people using a computer, you can create an account for each one.

User accounts are critical because they separate your files, and sometimes programs. This is good for privacy and security, as long as each account has its own password.

However, what many people don't know is that there are multiple types of accounts you can create. The two major ones are "administrator" and "standard."

You'll want to check your user accounts right away and change any administrator accounts to standard accounts.