Ten insider ways to keep hackers and scammers away from your private files

By Francis Navarro, Komando.com, June 9, 2018

Cybercriminals are always looking for ways to steal your personal data. We've seen a huge uptick in the number of data breaches over the past few years. It's not always your information that the criminal is after though. Sometimes the thief is just looking to steal your gadget, for either personal use or to sell for profit.

It's enough to make you feel like protecting your information is practically impossible. But that's the wrong way to look at it. As the services we use on a daily basis become larger targets for hackers, that means it's even more critical that we all take the necessary steps to protect our private data.

With cybercrime so rampant these days, you need to be proactive about protecting yourself. To help you out, here are 10 insider ways to keep hackers and scammers away from your private files:

1. Keep your software, firmware and operating systems updated

If you want to keep your computer safe (and get the latest features, too), it's important to install the updates as soon as you can, especially if they're aiming to fix security bugs and issues. Keep all your apps, smart appliances and even your router updated with the latest patches and firmware too.

If hackers can find a flaw in a program or operating system, they can actively use it to attack computers until it gets patched. These types of flaws are being pursued relentlessly by hackers and software developers try their best to keep up.

And perhaps the scariest type of flaw is the zero-day exploit. Zero days are flaws that hackers are already exploiting, without the software developer's knowledge. Even worse, since they're unknown, zero-day flaws often let hackers get around your security software with no input from you.

Obviously, it's important to update these programs, and any other programs you use, whenever patches are available.

2. Secure your devices

If you think about it, our computers and smartphones hold so much information about us. These gadgets know who your contacts and friends are, they save snapshots of our lives through photos and videos, they keep track of where you are, they know your browsing habits, your financial transactions, and your shopping habits; your gadgets know virtually everything about you!

But how secure is your smartphone or computer against would-be snoopers and hackers? I hope you're using some kind of security system on your gadget to protect your privacy.

Surprisingly, over one-third of smartphone users don't even bother to use even the simplest 4-digit pass code to secure their gadgets. Even worse, a survey showed that about 70 percent of the participants do not use any security protections for their computers at all.

Now, these are security lapses that you shouldn't ever do. At the very least, have a strong password or passcode to lock your gadgets and lock them whenever you're away.

Currently, there are a number of ways to lock and unlock our phones and tablets - face scans, thumbprints, irises, passcodes, patterns, and more. On desktops and laptops, aside from the old login password system, biometric systems like fingerprints and face scans are also becoming commonplace.

3. Use a firewall and anti-malware protection

One essential tool that keeps hackers from seeing your computer online is a firewall. Even if they 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? Well, newer Windows and Mac systems all have built-in software firewalls for configuring your outgoing and incoming internet ports. Although useful for certain applications, you have to be careful when tweaking your firewall port settings.

A wrong port setting can leave your computer vulnerable to port scanners, giving hackers an opportunity to slip past. Also, if your computer has been exposed to a virus, it might have changed your port settings without you knowing.

Here's how to test your firewall to make sure it's working.

Another thing that will protect your system from spyware and remote access malware is security software.

Good security software will keep 99.99 percent of viruses out of your system and let you focus on avoiding the big threats instead of sweating the small stuff. Whether the virus is in a download, email or coming at you online, security software can detect and block it.

There are plenty of security software programs, some free and some paid. If you're running Windows 8 or 10, you may have noticed that your system already has built-in antivirus and malware protection software called Windows Defender. It's actually a decent program for guarding your PC against virus and malware threats.

Other free options include Avast and AVG. However, while they do the basic scanning and protection well, they aren't going to have the range of extra options that a paid option might, such as an added firewall, parental controls, website reputation monitoring or protection for multiple gadgets from one place.

For these features, you can look at paid options like Symantec or Norton.

Note: If your computer has a virus, you could lose all of that data! Protect every device you own with a solid backup service from our sponsor, IDrive! Plans start at just $5.95 per month for 1TB of storage. And as a Kim Komando listener, you can save even more! Click here to save 50 percent on 1 TB of cloud backup storage!

Of course, installing security software doesn't help much if you never update it. Hundreds of new viruses are released every day and updates help your security know what's dangerous and what isn't.

4. Use encryption

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.

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.

Note: To set up FileVault, click the Apple menu and select System Preferences. Then click the Security icon. Open the FileVault tab. Now click Turn On FileVault.

Solid-State Drive (SSD) manufacturers also include management, encryption and secure deletion tools with their disks to make sure you check these available options too.

5. Beware of public Wi-Fi

If you've been following Komando.com, listening to The Kim Komando Show and subscribing to Kim's popular podcasts, then you know all about the major risks you're taking each time you go online. Those risks can even be greater when you're accessing the internet using 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.

Still, even though the risks are so high, many people use public Wi-Fi networks to check their bank accounts, purchase merchandise and complete other tasks that they'd prefer were private.

If you're not careful, cybercriminals can walk away with your name, address, Social Security number, email address, and even your username and password.

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. Web traffic is also encrypted, meaning not even your internet service provider can see your online activity.

We recommend FREEDOME VPN from our sponsor F-Secure.

Click here to learn more about our sponsor FREEDOME VPN and use discount code KIM to save 20 percent at checkout.

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

You don't throw away your personal files, credit card statements and tax filings in the trash for anyone to find, do you? If you don't do that to your physical files, then why shouldn't you do that to your sensitive digital files too?

Just like a physical 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 personal security, you need to erase sensitive data for good. You get can rid of that personal data by using software tools like Eraser or Blank and Secure for Windows and Secure Delete - File Shredder for Macs.

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

Click here to learn how to safely delete data forever on your PC or Mac.

Do you want to take it a step further? Software solutions may delete your data forever, but there's a certain satisfaction to be found in physically destroying it in addition to wiping the data.

Click here for three ways to destroy an old hard drive.

7. Always use strong and unique passwords

Thanks to online banking, social networking, and the cloud, much of your digital life is now online. Hackers would love to get access to any of your online accounts so they can steal the information you've uploaded.

Your password is the first line of defense against this. You want to make sure you set up a strong, unique password for every account. That way, it's hard for hackers and their computers to guess. If your password is revealed in a breach at another site, it won't give hackers access to every account you have.

Click here for a simple trick to creating a strong, easy-to-remember password. If you're feeling overwhelmed with passwords or want to create harder passwords, consider using a password manager.

A password manager 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 own personal key.

For your password management needs, we recommend our sponsor LastPass. It's one of the most popular password managers out there for a reason - it's one of the best and easiest to use.

Learn more about how our sponsor LastPass can help you at home and at a work. Click here to get a free LastPass Premium 30-day trial!

8. Use two-factor authentication

I'm talking about turning on two-factor authentication (2FA) for your accounts. Two-factor identification is a fancy name for adding an extra verification step to the login process of your most critical accounts.

With the 2FA setting enabled, 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 special one-time code that's texted to your cellphone.

The idea is that even though hackers may have figured out your credentials, without the special code, they still won't be able to access your account.

This gives you an extra strong layer of security because it's unlikely that hackers have physical access to your smartphone too. Click here to read more about two-factor authentication.

9. Secure your Wi-Fi then turn on your guest network

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 just 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 main network, preventing them from seeing your shared files and services. To avoid confusion with your main network, set up your guest network with a different network name (SSID) and password.

Although the guest network is available to guests, maintain the same level of security as your primary network. This means developing a strong password and restricting access to your shared files and devices. Make sure that "local access" is set to "off," which will prevent guests from tampering with your system.

Click here to learn more ways to keep strangers off your Wi-Fi network and out of your files.

10. Always use 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 important 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."

The difference is that someone using an administrator account can do whatever they want to Windows, including changing settings and installing new programs. Someone using a standard account can't unless they put in the right password.

That makes standard accounts great for kids or less-savvy users. However, in actual fact, everyone should be using a standard account. That way if a virus sneaks onto your system, it can't install without your permission, which makes you safer.

Additionally, malware typically assumes the permissions of the account it was installed with so using a standard account will typically minimize the damage done to your computer.

You'll want to check your user accounts right away and change any administrator accounts to standard accounts. Click here for step-by-step instructions. If you're running a Mac, here are some instructions for you.