8 bad online habits that expose you to viruses

By Christa Geraghty, Komando.com, September 19, 2019

Jumping through hoops, vaulting hurdles, and avoiding pitfalls in the landscape. While these skills make for great Olympic moments, they're more reminiscent of those computer users employ every day in the hopes of not winning gold, but to stay safe online.

The fact that it requires such a great effort to evade becoming a victim of computer-related crime is discouraging. However, it doesn't have to be exhausting. Simply changing some poor habits you practice while online will help ensure your computer and data are protected.

Although no amount of groundwork, guarantees a win against cybercriminals, with a bit of diligence and determination, you at least have a chance. Before you claim victory, it is essential that you eliminate the following bad online habits from your game plan.

1. Leaving your gadgets unprotected

Using antivirus software is the foundation from which all your other online safety habits are built. If you have chosen not to bother using anti-virus software, it is only a matter of time before you encounter issues.

Curious as to how harmful a computer virus or malware can be to your computer? Once infected, your system and data are comprised and can be destroyed in mere seconds.

The good news is if you have a Windows desktop, you already have one of the best anti-virus programs built-in, Windows Defender. In addition to scanning your system frequently, it is crucial you keep current with system updates to ensure your anti-virus program is ready to defend against the latest malware.

2. Only relying on anti-virus software

While experts work diligently at developing software that protects against viruses, criminals are always upping their game. This constant cat and mouse race leaves even the best anti-virus program shy of being able to protect your system 100%. Because no single security solution is perfect, it's essential you practice other good online habits.

Historically, running *two* antivirus programs was considered a bad idea, because of potential conflicts. Windows 10 allows you to run whatever antimalware program you choose, and optionally leave Defender in place to periodically check for threats as a secondary measure. (Go to *Settings* > *Update & Security* > *Windows Security*, then click on *Virus and threat protection*. Scroll down to *Windows Defender Antivirus options* and make sure *periodic scanning* is toggled on.)

3. Public Wi-Fi isn't your friend

We are all guilty of this bad habit at one point or another. You are on the go and need to get online, so you quickly connect to a local public Wi-Fi. Unfortunately, taking advantage of 'free' Wi-Fi may cost you, as public Wi-Fi networks are unsecured and easy to hack, leaving your system and data vulnerable.

Since this type of network is open for use by anyone, there is a high risk of exposing your system to malware and having the information you send or receive, including passwords, viewed and collected by criminals. Of course, refraining from using public Wi-Fi is highly recommended.

However, for those occasions when you need to access the internet and are away from a secure wireless network consider installing and using a virtual private network (VPN) which supplies an encrypted connection from your device to a network across a public network.

The encryption safeguards against unauthorized persons from accessing your data while it's being transmitted. Our sponsor, ExpressVPN, supplies the security you need when going online and can be used across all of your devices.

4. Never ignore updates

Are you notorious for rescheduling software updates endlessly? If you often hit the 'Remind me later' button you are asking for trouble as this habit prevents your system or individual applications from getting the latest tools and security patches needed to fight off attackers and viruses.

While you may consider updating as inconvenient and time-consuming, you can schedule it to process during periods you are not on your computer. Most operating system updates contain security patches that help keep your device safe, so it's always a good idea to stay updated.

5. Emails from unknown senders could cost you

More than half of all email is spam. These unsolicited and unwanted pieces of junk find their way into every inbox as hackers have become very adept at crafting legitimate-looking emails; so much so your email program cannot always detect them.
To protect yourself from becoming a victim of a phishing scheme or infecting your computer with malware, ransomware or other threats, never click on attachments or documents inside unless you've verified the sender is legit.

6. Reusing passwords

This habit may be hard to break, but it is necessary. Sure it's easy to come up with a password you can remember and use it over and over again for every application or website. However, this practice can have severe consequences for you and your data.
With little effort, a criminal can decode your password and gain access to other accounts you use it for. Not only does this scenario leave your system vulnerable to malware, but it also exposes your information to attackers.
One resolution is to implement two-factor authentication, or 2FA, which requires you to enter another form of identification before you are permitted access to your account. Typical types of authentication include passcodes, passphrases, and biometrics.
Another method to increase security is to create unique passwords for each account. To help you remember your variety of newly minted passwords try making a list or spreadsheet to store them or use a password manager such as RoboForm.

7. Forget to clean up online accounts

It's common to have a ton of online accounts. Unfortunately, over time, you may forget about a few here and there leaving your password in danger.
To help prevent your information from being comprised, jot down all the accounts you have created and routinely go through and delete those you no longer utilize. When the inevitable data breach is announced from a site you no longer use, you'll be glad you did.

8. Not reading the terms of use

Just like everyone else on the planet, you skip right through the terms of use or End User License Agreement (EULA) when installing software or an app. The problem with this habit is that companies collect data from installed products and your usage.
Sadly, because you didn't bother with the fine print, an unknown amount of your information has been collected and stored in an unsecured database, waiting to be breached. Read or inquire about a company's data-collecting policies before installing any software or app.
By no means does this list cover all of the measures you can take to help ensure the security of your system and data. However, changing even a few bad habits, into good proactive routines will go a long way in the battle against viruses and other cybercrime.