

10 Tips to Securing Your Computer

November 30th is International Computer Security Day #ComputerSecurityDay and is an annual awareness day, started in 1988, that focuses on computer security. We all know that new viruses are created daily, hackers are always trying to steal information, and your computer is always under assault through the internet. Official or not, Computer Security Day is an excellent observance to remind us of these issues and encourage one another to be proactive in our computer use. The following are ten tips to help you secure your computer and avoid being the latest casualty in this never ending battle with the dregs of our cyber-connected world.

1. Software Updates

Software is inherently susceptible to hackers. When programmers work in teams to create software, they leave holes (backdoors) in the lines of code to easily navigate, to allow others to insert additional lines of code as needed, and to allow the linking of separate distinctive routines. There are essential in programming; software production is nearly impossible without them. Unfortunately, when the software is ready for production, many of these holes are missed or forgotten and the software is mass produced with vulnerabilities. Software patching and updates are commonplace in the industry and if you do not install these updates or patches when they are released, your software is at risk of being compromised by hackers and viruses.

2. Anti-Malware Software

In a 2018 report, it was estimated that an average of 959 new malware infections emerged every hour in the year 2017¹. That was up by nearly 23% from the previous year. More importantly, these infections are no longer strictly limited to viruses like in years past, malware refers to any malicious software including Trojans, worms, spyware, adware, ransomware, scareware, and, yes, viruses. Today's computers are under constant attack by those who would wish to do your computer harm and steal your personal information. It's essential that you are running a good anti-malware package and update it on a regular basis.

3. Good Passwords

Using the old standby passwords like "12345678" and "password1" is not good enough. You need to use effective and complex passwords to protect your information. It seems like every time you go to a new website, you need a new password. It can be overwhelming but these passwords are extremely important in securing your identity and personal accounts. A good password contains upper case letters, lower case letters, numbers, and non-alphanumeric symbols. One way to create memorable passwords is to use a phrase and

¹ (Benzmuller, 2018)

transform it using non-conventional characters. For example, Cathy's Facebook Account may use a phrase like "Cathy Loves A Secure Facebook In 2018" and can be transformed into a password like "C@thyL0v3s@\$3cur3F@c3b00k!n2018".

4. Downloads

When surfing the internet, you're very likely to get popups encouraging you to download something – just don't! Never download anything on a whim. If you are looking for a specific piece of software to download, first go to the manufacturer's website. Third party websites that host download links to another third party website are pretty common and many are highly disreputable. Also, only download from a website that you are familiar with by their web address or url address. Sometimes, criminals will spoof a legitimate website with an illegitimate or fake website. Always look carefully at the web address where you are looking to download files; www.bankofamerica.com and www.bankofmerica.com are not the same.

5. Keep Personal Information Safe

Your personal information can be the key to hacking your bank account, social media accounts, or credit cards. Don't indiscriminately give out too much information. When asked for identifying information, always know to whom you are giving that information, and don't offer up too much information on your social media pages. Sometimes it's good to be a bit of a mystery. Like download pages, be very careful when filling out information requests on a website and make sure the website that you're on is the one that you really want to be on. Remember web-based information forms are easier to mimic online than the whole website.

6. Scan Email Attachments

Always be careful with email. Not everyone who sends you email is your friend. Spam accounted for over half of all email sent in the United States so far this year.² In the global community, some estimate that number to be nearly 70%. If you receive an email that looks suspicious with grammatical errors or unnatural phrases, delete it. If you receive an email with an attachment, scan it with your anti-malware software before opening it. If you receive something from a friend or business associate requesting something that's unexpected, call them directly, ask if they sent it, and provide the information directly.

7. Screen Lock

When you leave your computer, particularly in a public area or workplace, lock the screen with a password. It's so inconvenient to lock your computer screen but if you're leaving your computer up and going to lunch, any one could easily sit down in your chair and use your computer to access your information, your accounts, and your saved websites. Your computer password should also be a good password and not easily "guessable".

² (Vergelis, Demidova, & Shcherbakova, 2018)

8. Log Off Completely

Particularly on public networks, you should never just close your computer and leave it connected. Public networks are high susceptible to hackers and by leave your computer on those networks, you're leaving your system open to anyone with some minor skills to "steal" anything on your computer. Also be very careful in public places with prying eyes. Be careful of your surroundings and, if at all possible, sit with your back to a wall with your computer screen facing you and the wall.

9. Backup

The most important thing on your computer is your data. Make sure you have your files, pictures, and documents in three locations: your computer, your backup, and one more place (another backup, the cloud, a file server, etc). If all else fails and your computer is lost, stolen, dies, or is run over by a truck after you pull out of the parking lot with it on the roof of your car, your data can be restored from a backup. There are also system image backups that create a clone of your computer as it sits. These system images can be restored to a replacement system including, not only your data files, but even your programs, shortcuts, and settings. Some people consider Dropbox, iCloud, and the like to be a backup but they aren't. If a file in your Dropbox or iCloud is deleted, it is also deleted in your Dropbox or iCloud folder on your computer. A true backup allows you to recover files that have actually been deleted intentionally or accidentally or even pull a copy of a file as it was two weeks ago without any changes you may have made in the meantime.

10. Preventive Maintenance

Just like getting your car serviced regularly, your computer needs preventive maintenance as well to keep it running smoothly and efficiently. You should remove old unused programs, clear your temporary internet files and cookies, cleanup your system registry or disk permissions regularly. You should also perform regular physical cleaning of your computer. Clogged fans and vents prevent proper cooling which can destroy the sensitive electronic components in your computer and that sticky keyboard and screen are just gross. Proper preventive maintenance and replacing components as they age can significantly increase the lifespan of your computer.

Benzmuller, R. (2018, 03 27). *Malware Numbers 2017*. Retrieved from G Data Software Security Blog: https://www.gdatasoftware.com/blog/2018/03/30610-malware-number-2017?utm_campaign=Feed%3A%20GDataSecurityBlog%20%28G%20Data-SecurityBlog%29&utm_medium=feed&utm_source=feedburner

Vergelis, M., Demidova, N., & Shcherbakova, T. (2018, 08 14). *Spam and phishing in Q2 2018*. Retrieved from Kaspersky Securelist: <https://securelist.com/spam-and-phishing-in-q2-2018/87368/>