Security tips for computers and laptops

The computer (or laptop)[1] is a ubiquitous item in most households. It sits in the corner for the kids to do their homework on or for us to check email and maybe pay a bill or two. At the office, it is the workhorse that we don't even think about when we log in every morning and turn off each evening.

Computers can be a vulnerable technology that abusers can exploit to gain information about what a survivor is doing. While a computer may not be as intimate to us as a smartphone (yes, some of us sleep with our smartphones), it still contains a lot of personal information, from email accounts to web browsing activity, from filling out forms and documents to saving and storing important information. Whether you're setting up a new computer or just reviewing your computer's settings, here are some privacy and security tips.

The only way to completely prevent someone from accessing your computer is to keep it disconnected from the internet or other network (such as a home network even if it's not connected to the Internet), and put a passcode on your computer so that only you can access your computer. If you are concerned that someone might be getting into your computer, and you're comfortable with disconnecting it from the internet, this might be an option. For most people, however, disconnecting from the internet prevents them from doing what they need their computers to do.

PREVENTION AND PROTECTION

Here are some ways to minimise someone's ability to gain access to your computer.

Turn on firewall protections

Most computers and laptops (as well as tablets and mobile devices) come with firewalls already installed. Firewalls monitor data that is sent to and from your computer; when data with potential malicious software is detected, it will prevent that data from being communicated to your computer. Essentially, a firewall will protect your computer from someone who is trying to hack it through its open connections.

On most Windows operating systems, firewall protections are turned on by default, and you don't have to do anything. Mac and Linux operating systems have the firewall turned off by default, but you can turn it on. To see if your computer's firewall is on, check the firewall settings under the Control Panel (for Windows operating system) and System Preferences/Security & Privacy (for Mac).

[1] Although in this handout, we refer to computers, you can apply these suggestions to a laptop too.

Run anti-virus/anti-spyware software

To protect your machine from viruses and spyware, you should install and run anti-virus software. Anti-virus software will scan your computer and files you download for viruses, and if it detects any viruses, it will prevent it from installing. Some software may quarantine the virus to keep it from infecting your computer while others will remove the virus.

Anti-virus software relies on virus definitions to detect the virus; however, cybercriminals are constantly changing viruses to infect devices. For this reason, make sure your anti-virus software is running the latest definition. Most anti-virus definitions will update automatically. If yours do not, set up your anti-virus software so it does.

Anti-spyware is similar to anti-virus software, but it's specifically for spyware. If you're concerned that the abusive person might be installing spyware onto your computer remotely, running anti-spyware can be helpful.

Anti-virus and anti-spyware software will not completely prevent malware from being installed. However, it will increase your computer's protection. There are many free anti-virus/anti-spyware products available for the home user. Google "best free anti-virus or anti-spyware" for the latest reviews.

Turn off remote access

If you're worried about someone remotely accessing your computer, either legitimately or without your permission, you can turn off its ability to allow remote access. You can always turn it back on if you need remote access to your computer.

How you turn off remote access on your computer depends on the operating system you are running. On a Windows computer, you want to turn off the setting that says: "Don't Allow Remote Connections to this Computer" (generally found under the Control Panel). If you have a Mac, go to System Preferences/Sharing, and uncheck "Remote Login" and "Remote Management." The best way to find specific instructions for your computer is to Google "how to turn off remote access to [your operating system (e.g., Windows 10)]."

Disable file sharing

If your computer is connected to a network (even if it's not connected to the internet) other devices that are connected to the same network could be able to access the files on your computer. This may be a concern if you're connected to a public Wi-Fi network and you have your settings set up to share. If you don't need someone else to have access to your files, disable file sharing.

How you disable file sharing depends on the operating system you're using. The best way is to Google "how to disable file sharing on [your operating system (e.g., Windows 10)]". For most Windows operating system, the setting will be under the Control Panel, and you want to "turn off file and printer sharing." For a Mac, go to System Preferences/Sharing, and uncheck "file sharing" and "printer sharing."

Use non-admin account for everyday use

Some malware and "hacks" require administrative access to your computer. This means that if you're signed in as an administrator on your computer and accidently click on a link that has malware embedded, it will download and install. However, if you are signed into your computer as a non-administrator and set it up so that a non-administrator account cannot install software, it won't install even if you accidentally click on a link with malware.

It is, therefore, helpful to create a non-administrator account on your computer for everyday use. You can always log in on the administrator account if you need to install software or make changes to your computer. Both Windows and Macs allow you to create multiple users.

GOOD PRACTICES FOR COMPUTER SECURITY

In addition to computer settings that you can turn on or off and running software to help protect your computer, there are other good practices that you can use to increase your computer's security and your privacy.

Put a password on your computer

Locking down your computer with a password is the first thing you can do to prevent someone from gaining access to your content. While most people are worried their computer will be "hacked," the easiest way for someone to gain access to your computer is simply by having physical access to it, either because they are in your home or have stolen it.

Don't click on unknown or suspicious links

Another good practice is not to click on links or attachments from suspicious people or websites. Because malware can sometimes be embedded in these links or attachments, "opening" one could install the malware. If you need to receive files or open links from an abusive person or someone you don't trust, consider using a cloud sharing service to share files or communicate the information in another way.

Log out of accounts and quit programs

When you finish using an online account, a program on your computer, or even the computer itself, quit and log off. Leaving accounts and your computer logged in could make it easier for someone else to get into your accounts. Even if you don't think someone has physical access to your computer, it's always best practice to log out when you're done.

Turn off access points when not in use

Turn off WiFi, Bluetooth, Airdrop, or other connectivity access on your computer if you're not using it. If the access point isn't open, it will be harder for someone to connect remotely. You can always turn it on when you need to connect.