Safety from viruses and malware on your computer

Key take-homes:

1. **Keep your operating system up to date.** Yes, those nagging reminders are annoying, but don't put off doing the updates. If you have a PC and aren't running Windows 10, take special precautions. Most viruses are targeted towards PCs, so Windows users need to be careful.

2. **Use extreme caution when installing software**. Macs make it difficult to download software from unapproved developers. On PCs, software from commercial vendors is relatively save. On both platforms, do not install software unless you trust the developers and have retrieved the software from a reliable download site. Some "free software" websites that provide legitimate software are nevertheless designed to trick you into clicking on the wrong thing and downloading legal adware that you didn't intend to install.

3. **Don't click on links in emails**. It is very easy to impersonate a sender and to make an email look like it came from your bank or some other trusted sender (a phishing scam). It's better to log in to banks and commercial websites via a bookmark or by typing in the URL. If you do click on emails in links, always mouse over the link and make sure that the URL shown is the actual website you want to go to. At Vanderbilt, Outlook scans links in emails to block unsafe sites. However, this system makes it difficult to know the actual URL of the link.

4. **Back up your computer**. The best protection against ransomware (which makes your data unavailable by encrypting it) is to back up your computer to the cloud or removable media. This will protect you against hard drive crashes as well!

5. **Avoid sketchy websites**. You are unlikely to get a virus from visiting reputable websites, such as Wikipedia, well-known news sites, YouTube, Facebook, Amazon, etc.

6. **Change default passwords to strong passwords.** Many people use devices like WiFi routers, security devices, etc. without changing the default passwords, making them vulnerable.

7. **Don't share memory sticks**. Viruses can be spread through flash drives so avoid putting yours in someone else's computer or using someone else's flash drive in your computer. This method of spreading viruses has become less common as more files are stored on the cloud.

Frequently asked questions:

Can Macs get viruses? Yes, they can, although there are a lot of built-in features that make it less likely than on Windows. Nevertheless, be sure to pay attention to any warnings you see when you download files or install software.

Do I need to download virus scanning software? If you are running one of the current operating systems (Mac OS 10 or Windows 10), you probably don't. On Windows 10, Windows Defender is now build in to the operating system and should automatically update virus signatures. The Mac OS has a built-in scanning too (Xprotect) that works automatically in the background. Windows operating systems prior to Windows 8 are vulnerable and shouldn't be used without running anti-virus software.

What's the difference between a virus and malware? Malware is a general term for malicious software and includes viruses. Malware can actually be legal - those terms of use that you click on before installing may say that you agree to be targeted with a lot of unwanted ads (adware). A virus secretly spreads itself through the system by replicating itself and attaching to other executable files. Viruses can monitor your activity and steal your passwords and data (spyware), lock your data by encrypting it (ransomware), or frighten you into providing data or paying for unneeded software (scareware).

How can I know if I have malware? Windows Defender scans your computer periodically and reports suspicious files that it finds. You may discover that your computer is infected when an unusual window pops up. When computers are infected to mine Bitcoin, you might notice your computer running very slowly, getting unusually hot, or the cooling fan running more frequently than normal.

Can I get a virus from a Word document? ... a picture? ... a PDF? In order for malware to infect a computer, it must be "run" as an executable file. Both Word and Excel have the capability to run macros (utilities that run when the document is loaded), so they have the potential to spread a virus if macros are enabled. Pictures such as JPEF and PNG files are just data and are not executable, so they can't spread viruses. However, an executable file might be named in a way that makes it appear to be an image, particularly if your computer does not display file extensions. PDF files can include executable code such as Javascript, but an up-to-date PDF viewer will generally warn a user when such code is detected.

What should I do if I think my computer is infected? The best thing to do is to get help immediately. If you are connected to the network by a cable, unplug the cable. If your laptop has a hardware WiFi switch, turn it off. Advice varies as to whether you should turn the computer off. Vanderbilt IT advises leaving it on.

If you are affiliated with Vanderbilt:
- faculty and staff should get help from their local IT support personnel
- students should contact the VIUT help desk

If you are not at Vanderbilt:
- check with your IT department for work computers
- check with a reliable vendor for personal computers