Malware, Viruses, and Hacks

By John Tan

Malware, short for *malicious software,* is a blanket term for viruses, worms, Trojans and other harmful computer programs hackers use to wreak destruction and gain access to sensitive information. These viruses can remove access to your computer and may require an IT professional to re-enable your access. Contrary to popular opinion, malware affects not only PCs but also Apples and Androids (Google it if you don't believe this).

Viruses can be spread through email and text message attachments, Internet file downloads, and social media scam links. Mobile devices and smartphones can become infected with mobile viruses through shady app downloads. Sophisticated hackers that can gain access to your computer or device.

Some examples when your computer is being compromised: when your mouse starts moving around without your intervention, a browsing window suddenly changes to other pages, or your login password is changed and you can't log on. *Immediately shutdown or power off* whenever this happens. A computer *left on "if" there is a hacker, will gain knowledge and access to personal and financial information*. It only takes a few minutes for them to take advantage of the situation. Press the power button until the power shuts down.

Installation of free or purchased malware virus protection software is recommended. Malwarebytes, Norton Anti-Virus, AVG, McAfee Anti-virus programs are a few. Set up properly they will run in the background of your computer and check for malware.

There are basic and advanced settings within the malware programs to protect your computer. "Automatic update" setting will keep the program up to date. Almost every anti-viral program that you use will have new definition (program) regularly updated. These updates basically give the program to check for new-found viruses out in the internet world. Unfortunately this process does not guarantee that your computer is 100 % virus- free, as new viruses are created every day. It's a catch-22 scenario, but at least you have some type of software to counter-attack the known viruses and malware.

Some of these companies will let you try out a 30-day trial version with an option to buy a maintenance plan or a monthly or yearly subscription. You can find these products and many others online from your favorite browser or built-in application store: Apple, Google, Android stores or do a search online. Ask your local computer technician or store for their recommendations, if you are unsure what to use.

If your computer is compromised (no access) you should take your computer to the nearest computer repair shop for them to diagnose the problem. They usually have software tools and

special login restart commands that they'll be able to gain access to your hard drive.   It's not 100 % a guarantee, as hackers can disable many background functions that computer technicians normally use, and make it nearly impossible to get your computer back up to normal. This is a reminder to always BACK UP your data. For more information and resources, visit www.oakmont-learning.org.