PROTECT YOUR COMPUTER

The first step to preventing malware infections is to install and maintain security programs on your computer. While computers can still get infected with security programs installed, an unprotected computer is at much greater risk.

1) UPDATE SECURITY PROGRAMS

Always remember you have **three** security programs to update: Windows Updates, your anti-virus protection (McAfee VirusScan, Norton, etc.), and Malwarebytes. Keeping these up to date is most important when your computer is off campus: about **half** of the malware infections cleaned by the Computing Help Desk are reported in the first two weeks of the semester. Your computer is at risk when any one of these security programs is out of date.

2) SET UP AUTOMATIC SCANS

Your computer may still be at risk even if your security programs are up-to-date. **Schedule** Malwarebytes quick scanning to catch malware infections early on. It is also a good idea to do a **full scan once a month** in both Malwarebytes and VirusScan.

3) PROTECT YOUR WEB BROWSER

Update to the latest version of Firefox and download the AdBlock Plus extension. AdBlock Plus blocks irritating advertisements which sometimes contain malware.

4) UPDATE WEB-RELATED PROGRAMS

Some programs are used within web browsers like Firefox and Internet Explorer. Because these programs are used on the web, they can be a **security risk** if they are not updated. Adobe Flash Player, Adobe Reader and Java should all be **updated regularly** from the Adobe and Java websites.

WATCH YOUR HABITS

Security programs go a long way toward protecting your computer. However, **you are your own best protection.** *Being a cautious and aware user will do the most to protect you from malware infections.*

5) LOOK BEFORE YOU CLICK

Everyone knows that clicking on links willy-nilly is a quick way to get malware. However, malicious links aren't just in emails anymore. Malware can send malicious links that appear to be from friends through **chat clients** like Google Chat, AIM and MSN Messenger, and in **messages**, **groups**, and **fan pages** on social networking sites like Facebook, Twitter and MySpace. **When in doubt, just don't click.**

6) KNOW YOUR COMPUTER

You spend more time with your computer than any textbook or piece of equipment. **Know which programs are installed** on the computer, including the details of your anti-virus and anti-malware programs. Warnings or messages from **unfamiliar programs** may be from partially installed malware trying to finish the job. Many infections are the result of clicking OK on a message that wasn't fully read or understood.

7) TAKE THE BEATEN PATH

The less familiar you are with a website, the more careful you should be when browsing. Try to only visit sites you trust. Don't click on ads or suspicious links. New websites and video streaming websites like sidereel.com and surfthechannel.com are often less secure than bigger, more well-established sites.

8) DOWNLOAD WITH CAUTION

Everyone knows that downloading copyrighted content from websites that aren't authorized to share it is copyright infringement. Did you know that these downloads also open up your computer to malware infections? Peer-to-peer programs like LimeWire, uTorrent, Vuze, and Ares Galaxy have such poor security that **people can use them to infect or remotely access your computer, even if you aren't actively using the program.** Free video streaming websites sometimes require you to install a special player that may contain malware. Additionally, a large number of downloads and torrents actually contain malicious code. **If you didn't buy it, don't download it**.

BE RESPONSIBLE FOR YOUR DATA

Despite good browsing behavior and consistent security updates, something may go wrong with your computer. Follow these steps to save time and ensure your own peace of mind.

9) THE DEVIL'S IN THE DETAILS

The more information you have for the Computing Help Desk when your computer gets infected, the faster they can help you. Complete and detailed error messages, the duration of the problem, specific symptoms, and what you were doing when you first noticed the problem are all very useful things to know when troubleshooting an issue.

10) BACK THAT THING UP

If all else fails, the Computing Help Desk may have to have to reformat and erase all the data on your computer. Sometimes they will not be able to recover data from the computer before they erase it. Frequently backing up your data saves time and saves you from losing irreplaceable photos and important documents.