Resources for Online Learners

Computer Viruses and Data Security

What Are Computer Viruses and Why Are They Harmful?

Viruses are an unpleasant fact of computing life. Tens of thousands of individual viruses had been identified, and new ones are being created all the time.

Some of these viruses are *worms*, sets of instructions that replicate themselves over a computer network and use up the computer's resources, often shutting the system down.

Macro viruses are spread through shared documents. Many applications, such as Microsoft Word and Excel, support powerful macro languages to streamline complex or repetitive tasks. These applications allow you to embed a macro in a document, and have the macro execute each time the document is opened. Once a macro virus gets onto your machine, it can embed itself in all future documents you create with the application. According to some estimates, 75% of all viruses today are macro viruses.

Boot sector viruses are especially dangerous, since they erase or modify critical portions of your operating system, making your computer inoperable.

Some viruses can be destructive without harming any particular computer. Circulated as an e-mail attachment, the *melissa* virus was downloaded from the Internet by numerous unsuspecting computer users, where it replicated and e-mailed itself to the first 50 people in each user's address book. The resulting exponential growth of *melissa* tied up Internet traffic around the world. Other viruses can be relatively harmless but very annoying.

Before the ~~recent~~ NIMDA virus, infection by e-mail virus required the user to open an attachment (e.g., a contaminated document file). If the contaminated attachment was an executable file (.exe file, .dat file, .bat file, etc.), you had to double-click on the file, or save it somewhere and select "file...run..." to activate the virus. However, the NIMDA virus could be activated by merely reading an infected e-mail message, proving that we must be careful before opening ANY mail online. Even though Western University is set up to block viruses and executable files downloaded through the campus e-mail server, getting into good habits when dealing with incoming messages and files will help you avoid contaminating your personal computer system in the future.

You wouldn't eat an old piece of candy you found lying around somewhere, would you? So why would you read a message from an unknown source or run an unfamiliar attachment, not knowing what it was or where it came from? Curiosity, maybe--but we all know what that did to the cat. **The best way to avoid contamination from computer viruses is to avoid opening e-mail messages or running files you receive as attachments, unless you know exactly what they are.** Keep in mind that even if you receive a file from someone you know, you may not know where that person got the file.

Keeping Your Computer System Free of Viruses

If you have reason to believe you have a computer virus in your system, the first thing you need to do is find out more about it. Select a search engine like Google and run a search on the name of the virus.

As a WesternU student, you should have a current version of an anti-virus program installed on your computer. Laptop computers issued by the University already include antivirus software. You can download similar software to your personal computer from the Web.

If you are installing your own virus checking software, keep in mind that the free trial versions offered by McAfee, Norton, Symantec, and other antivirus companies are NOT sufficient. It's worth the price to get a registered version, along with periodic updates as new viruses are discovered. The program can also be used to check any individual files you receive before you run or open them.

Because new viruses and worms pose an ongoing threat to your computer system, **it's important that you update your virus definitions at least once a week, preferably daily**. Some virus checkers automatically update virus definitions on a regular basis, or at least alert you when it's time to update the definitions manually. In most cases, you can do this online by going to the Web site of the virus checker vendor and following the instructions there for downloading new virus definitions.

Be aware that while these virus checker programs are very useful in identifying and removing most bugs, they are not foolproof. Some viruses are actually legitimate macro programs, and won't be flagged by such programs. The best way to reduce your risk is to just *be cautious* and don't open or run unknown programs. If you get one from a friend, but don't know what it is or where it came from, ASK!

Avoiding Infection Through CDs and Floppy Disks

Another route of virus entry is the floppy disks that you get from friends or colleagues. Commercial CDs are usually safe, as they are usually created in virus-checked conditions, and can't be written to again. *Rewriteable* CD's provide no such guarantees. If you or other family members routinely exchange CDs or floppy disks with others, **make sure you have a virus checker program, and use it to check disks before opening or installing any files**. Checking the disks is like washing your hands in the clinical setting. You wouldn't eat dinner after a day at the hospital without washing your hands. Likewise, you shouldn't use *any* foreign disk without checking and cleaning it with a virus checker first.

Securing Personal Data with a Personal Firewall

While installing antivirus software is essential, there are additional steps that you can take to avoid other kinds of security problems. Every minute your computer is online, it is vulnerable to intrusions and information theft from hackers, regardless of the kind of Internet connection you have. These intruders can use eavesdropping tools to monitor your online activity, introduce code to disable your system, or run remote control programs that seize control of your computer.

Many of the same companies that offer antiviral software now offer personal firewalls that placs a barrier between the Internet and your PC, helping to block hackers from accessing your computer. Every time your computer is probed or attacked, you get detailed reports and clear follow-up options.

To summarize:

1. **Use caution when opening or running attachments**
2. **Get a virus checker program and use it**
3. **Regularly update your virus checker's virus definitions**
4. **Consider getting personal firewall software to avoid data theft**

Additional Resources

Dr. Solomon's Virus Solutions

McAfee's Virus Info Library

Symantec AntiVirus Research Center (SARC)

Virus Encyclopedia

Please contact **techsupport@westernu.edu** or **909-469-5432** if you have any questions regarding the contents of this document.