General

What is the best way to protect my computer from viruses, hackers, and malware?

Following the suggestions on this page will help you prevent major issues with your computer.

Use a virus scanner

Viruses are a hot topic in today's world, with many major outbreaks occurring each year. Most of these outbreaks could be prevented if people keep an up-to-date virus scanner running on their computer. Also, it is a policy at Florida Institute of Technology to require that all windows-based computers connecting to the campus network must have up-to-date virus protection.

There are many popular virus scanners available today, including McAfee Antivirus, Norton Antivirus. McAfee and Norton Antivirus can be purchased in most stores that sell computers for a nominal fee. AVG Antivirus is another widely popular Antivirus software that is available for free.

For your personal computer, you can find a link to AVG Free on our software page. Campus computers use McAfee VirsuScanÂ Enterprise.

For university-owned computers, McAfee Antivirus is used for Windows and Unix operating systems, and MacAfee VirusScan is used for Macintosh operating systems.

Installing an antivirus program is not enough. You need to keep it updated with the newest updates since new viruses come out all the time.Most antivirus programs update automatically after being installed. However, you should check from time to time to ensure that your virus definitions are being updated correctly.

To update McAfee, double click on the McAfee icon and click on the update button.

It is a good practice to update your anti-virus software weekly.

Use a firewall

Firewalls are pieces of software that restrict access to the network connection on computers. The purpose of a firewall is to make it impossible to access services on your computer that you do not use.

A lot of vulnerabilities today take advantage of flaws in common services that run by default on computers. Firewalls silently block access to these services preventing worms from attacking your computer - even if the vulnerability is unpatched.

Unix and Unix-like operating systems typically include firewalls built-in to the operating system. For recent Red Hat Linux installations, type the command lokkit from a command console, and select medium security. For other Linux distributions, search for information on setting up ipchains. If you are using a BSD operating

system, lookup configuration info on ipfw or ipf.

Most Windows operating systems do not include firewalls. The two versions of Windows that do include firewalls are Windows XP and Windows 2003 Server. These operating systems have very basic firewalls with very few configuration options, but they are still effective as a means to help protect your computer. It is recommended that you enable this firewall, as it is not active by default.

To enable the Windows XP / Windows Server 2003 firewall, follow the following steps:

Click on Start, and select 'Control Panel'.
Double-click on 'Network and Internet Connections'
Double-click on 'Network Connections'
Right-click on 'Local Area Connection' and select 'Properties' from the drop-down menu.
Click on the 'Advanced Tab' and check the box 'Protect my computer ...' and click ok.

If you do not own Windows XP, there are a number of software firewall titles available. These firewalls include Tiny Personal Firewall and Zone Alarm. Zone Alarm is free for personal use. Configuring firewalls such as Zone Alarm is no easy task, but they do include pretty good configuration options. For Zone Alarm, you will probably want to use the 'Medium Security' setting, since 'High Security' will block all programs from connecting to the internet by default.

Also, the personal edition of Zone Alarm cannot be used on university-owned computers due to the licensing restrictions of the software

In any case, you should look at the documentation that comes with firewall software before setting it up. Start out with a minimal-configuration for your firewall, and block stuff off slowly, so you can see the impact of your changes. If you have any problems accessing the network or web pages, you should first stop your firewall to make sure that is not the culprit.

Patch your operating system

New vulnerabilities are discovered every month in most operating systems. These vulnerabilities sometimes enable an attacker to take full control of your system, as was the case with the recent worms that attacked computers on campus in the late summer / early fall time frame. For these reasons, it is important to patch your operating system on a regular basis.

Although Unix-based operating systems usually don't have as many holes that allow attackers to take control of a system, they still have various vulnerabilities that are discovered on a regular basis - mainly third-party software products.

If you are using a Microsoft Windows-based operating system, updating your system is usually very easy. Just open up Internet Explorer, go to the 'Tools' menu and

select 'Windows Update'. Follow the prompts, and allow the 'Windows Update' activex control to run. You will want to install all of the 'Critical Updates'. Please note that this may require you to reboot your system several times during the process.

In addition to patching your operating system, if you use Microsoft Office, you might want to update that on a regular basis, as security vulnerabilities are found on a regular basis in the various utilities in Microsoft Office. To update Office, go to the webpage http://office.microsoft.com and click on the link to update your software. The update process is very similar to 'Windows Update'.

The procedure for patching Unix-based operating systems varies depending on the operating system. For Red Hat Linux operating systems, use the 'Up2Date' program to update your packages. Up2Date can be run by going to the Red Hat menu, selecting 'System Tools' and Red Hat Network. Using Up2date is pretty straight-forward. You may need to update Up2date to get it to work if you have an older version of Red Hat. You may download updated Up2date packages at the following location: https://rhn.redhat.com/

If you are adventurous, you can try the command-line version of the Up2date software by running up2date on a command console.

To update Debian and Progeny Linux, use the dselect utility from a command console. To update BSD operating systems, download patches from their respective websites. i.e. http://www.freebsd.org/security/

Clean adware and spyware from your computer

One annoying aspect of the internet world these days is the proliferation of Spyware/Adware. These nasty programs do things such as keeping track of what websites you visit while sending the information to a company, and popping up random pop-up ads. The majority of these pieces of software are installed by activex pop-ups in Internet Explorer. Other spyware/adware is installed as a part of other software such as Kazaa or Morpheus.

Some of the worst adware / spyware offenders include Gator, new.NET, Offer Companion, Bonzai Buddy and Comet Cursor. In order to scan for and remove these pieces of adware / spyware, download and install Adaware and/or Spybot Search and Destroy. Both programs sometimes find stuff that the other program doesn't, so you may want to use both. Spybot is free for anyone to use, but Adaware Personal is only free for personal use. As a result, Adaware cannot be used on any university-owned computers.

To combat the infection of spyware / adware on your computer, you can try a different browser, such as Mozilla or Opera, since most Spyware / Adware is installed via activex controls that only Internet Explorer supports. In addition, never install any program that you did not explicitly try to download. Pretty much all software that pops up a window asking you to install a piece of software that you did not ask for is spyware / adware. If a windows pops up asking you to install a

piece of software because it'll allow you to do things such as 'keep track of info you enter in forms', 'allow you to keep track of weather information for free', 'improves download speed' etc, click No.

Take action to protect yourself from email-based threats

In general, never run a .exe, .bat, vbs, wsh, pif, or .scr file you receive in email. Also, don't open any attachments in emails that look weird.

If an email asks you to forward it to 10 people for good luck, or tells you that you will receive money from someone just for forwarding it, delete it. You may also want to tell the sender of the message to stop sending chain-letters. These are all hoaxes and do nothing except fill up email boxes.

Also, don't believe virus warnings that cannot be verified. If someone tells you that a new virus is out, and that McAfee or Norton don't know about it, do not believe it. This is probably a hoax as well. You can visit McAfee's website: www.nai.com or Norton's website: www.symantec.com to lookup virus information. Always verify virus alerts yourself, before you take the chance of deleting a critical system file.

Reputable companies will never ask you for your username, password, credit card number or social security number via email. They will also never send emails wanting you to confirm a credit card number or password on a remote site. A company might have a problem with your credit card number if you ordered something from them, but in all cases, look at the site that you end up in your web browser. Real website will always include a valid domain name as the first part of the address, and will never contain an @ symbol in the web address. There are many scams going around right now that try to get AOL passwords, bank account information, Paypal account information, and credit card numbers.

For more information on various hoaxes and chain-letters circulating the internet, visit the following site: http://hoaxbusters.ciac.org/

Unique solution ID: #1091
Author: Tech Support
Last update: 2016-06-29 14:39