

Security Solutions



STUDENT TECHNOLOGY CENTER

Saginaw Valley State University
Zahnow Library • Second Floor

Your Tech-Know-How Place

Hours:

Mon 10 - 8
Fall and Winter hours
Mon 10 - 8
Tues 10 - 8
Wed 10 - 8
Thurs 10 - 6
Fri By Appointment
Sun 4 - 8

Spring and Summer hours

Mon 10 - 8
Tues 10 - 8
Wed 10 - 6
Thurs 10 - 6
Fri By Appointment
Sun 1 - 5

Contact:

2nd Floor * Zahnow Library
964-2299
techtutor@svsu.edu



Security Solutions

Security Solutions

This tutorial was designed to help you understand some of the security tools available that will enable you to better combat the many harmful items you can receive from the internet. The goal of this handout is that you will understand how to better protect your information using such tools and understand why you would want to use of these tool.

After completing this lesson, you should be able to:

- What Anti-viral tools are and where you can get them
- What is Spyware and how to fight it
- What are Popup Blockers and how they can help you
- What is a Firewall and where you can get one.
- What is Phishing and why you don't want to be caught in its net



Security Solutions

It is always a good idea to make sure that your computer is protected from the numerous nasty things that float around the internet. By using the following programs you will be able to better protect your computer.

Microsoft's Malicious Software Removal Tool – Removes various malicious items from your computer. <http://www.microsoft.com/security/malwareremove/default.msp>

Make sure you have Microsoft's Service Pack 2 - <http://www.microsoft.com/windowsxp/sp2/preinstall.msp>

Make sure your computer is fully updated.

Antivirus

Programs used to remove computer viruses and to protect from them. Always make sure your virus definitions are up to date. Also make sure you run your antiviral program regularly.

All computers that use SVSU's network (wireless or resnet) must have Symantec Antivirus installed on their computer.

Symantec Antivirus – SVSU supplies Symantec Antivirus to registered students.

Download location:

http://www.svsu.edu/support/index.cfm?doc_id=1904

Installation Instructions:

http://www.svsu.edu/support/index.cfm?doc_id=1903

AVG Free - <http://free.grisoft.com/doc/1>

Free Antiviral Software.

McAfee - <http://www.mcafee.com/us/>

Popular Antivirus program

Panda Software ActiveScan - <http://www.pandasoftware.com/activescan>

Online virus scan.

Symantec Web Scan - <http://security.symantec.com/>

Online virus scan.



Security Solutions

Spyware

These programs are used to remove many of the spyware that you can get from surfing the internet. It is wise to run these programs at various times just as you do with your antivirus programs and to also make sure they are updated. Both programs are free.

There are many programs that install spyware with the program when you install it. Some may stop working if you remove the spyware.

There are many spyware programs that are not actual spyware removal programs but spyware itself. A few of the legitimate and more popular programs are the following.

Spybot Search and Destroy - <http://www.safer-networking.org/>

AdAware - <http://www.lavasoftusa.com/software/adaware/>

CWShredder - <http://www.trendmicro.com/cwshredder/>

Removes the CoolWebSearch browser hijacking spyware

Popup Blocker

All major web browsers offer the ability to block popups. Many users use a third party piece of software to block popups. In Internet Explorer you need to go tools menu and then choose internet options. You will then choose the privacy tab and then you will see Pop-up Blocker at the bottom. You are then able to change setting along with turn it on and off.

Popup blockers can sometimes block popups that you may want to see or use. In these cases you need to make you turn them off or give access to that site.

Both the current versions of Internet Explorer and Firefox have built in popup blockers. If you wish to use another or don't wish to use one that is built into your browser the two following are popular popup blockers that also include other features.

Google Toolbar - http://toolbar.google.com/index_xp.html

Yahoo Toolbar - <http://www.yahoo.com/r/tb>



Security Solutions

Firewall

A firewall is a piece of software or hardware that stops certain communication between the computer and outside sources. This can help you from receiving attacks and access to your computer from outside sources.

ZoneAlarm - <http://www.zonealarm.com/>

Microsoft Firewall – located on Windows XP

Phishing

Phishing is the term for when people try to fraudulently acquire passwords, credit card information, or other personal information about you and do so by camouflaging themselves as a legitimate business.

Many time Phishers (The term of the people running the operation) will send emails and set up websites that look identical to real ones. You have a few ways to figure out if a site or email is legitimate or fake.

- Did a site such as paypal use your user name or did they address you as “Dear paypal user”. Many websites will always address you by your user name in emails to you.
- Did the credit card or bank give a partial account number? Most credit cards and banks will put a partial account number in emails they may send to you.
- Did the email contain information that only you should know?
- What are the address of the email and the address of the site it may send you to? Remember that even some legitimate email address and site addresses may look strange though.

Remember that these are not always safeguards and that people such as phishers are getting smarter every day. Sometimes the best ways to make sure you don't fall into their net is that you either disregard the email or contact the company itself and find out if



Security Solutions

the email is legitimate. Also using spam filters in your email will help restrict many of the emails that may end up being phishing scams

Just remember that many of the people who try to run email scams, create viruses, make spyware and may do other malicious things to your computer are always changing the way they operate and creating new programs. Make sure your programs are **always up to date** and that you are **aware** of the latest threats so you do not fall prey to one of them.