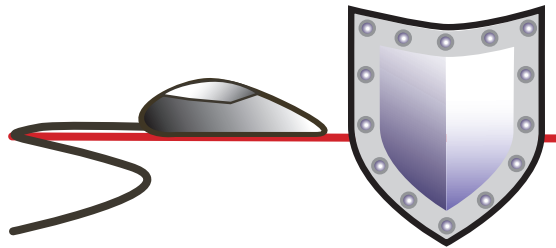


EVERYONE'S JOB

All computer users should take steps to increase security and reduce the chances of damage to you and your computer. Here are some common computer security issues and tips on how to keep your personal computer safe.



Spies & Unwanted Ads

Nobody wants their privacy invaded, but unfortunately unwanted spy software ("spyware") and advertising programs ("adware") can be put on your computer without your permission.



You can unknowingly install these programs on your computer by visiting certain web sites, downloading files from the Internet, or opening attachments in e-mail messages.



Spyware collects information about you and sends it to criminals using your Internet connection. Adware displays unwanted ads in pop-up windows or creates an ad bar on your computer screen.

Free or low-cost software is available to limit these intrusions.

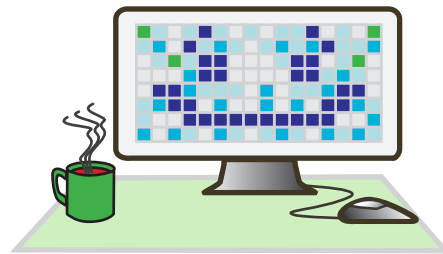
Getting Help

We have listed links to various resources on our computer security web page at: www.seattle.gov/informationsecurity/

Printed copies of this information are available by calling (206) 684-0600 or writing us at PO Box 94709, Seattle WA 98124-4709.

Help is available from computer technical support companies and online forums. Consumer Reports, computer magazines, computer stores, manufacturers and software companies can also provide useful information.

Your local public libraries and community technology centers are also great sources for more information. See: www.seattle.gov/tech/techmap/



This brochure prepared by the
City of Seattle

Department of Information Technology's
Community Technology Program and the
Office of Information Security(OIS)
www.seattle.gov/informationsecurity/
www.seattle.gov/tech/techmap/

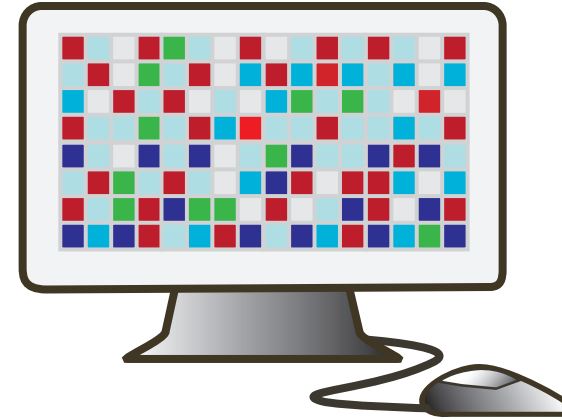
This information is provided for public education and awareness. While we have tried to make it as accurate as possible, we cannot ensure all information is correct and are not responsible for any errors or omissions.

We encourage you to do your own additional research and talk with trusted computer security professionals.

Version 6/2008



IS YOUR COMPUTER SAFE?

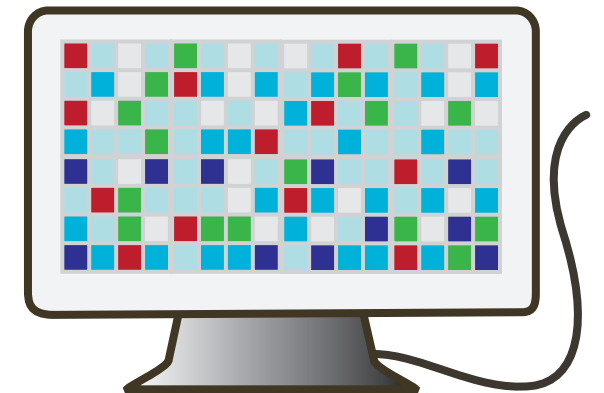


Tips for protecting your computer and your security



COMPUTER SAFETY:

Computers and the Internet are great. Unfortunately, home computers are also popular targets for criminals. Without proper protection, thieves can invade your computer and steal credit card numbers, bank account information, and other sensitive personal data. They can cause your computer to slowdown, stop working, or damage your files.



Viruses & Worms

Nobody likes catching a virus or getting sick. The same is true for getting computer viruses and worms.



A computer "virus" attaches itself to programs on your computer and causes harm to programs, information or hardware. A computer "worm" does the same and also reproduces itself. These can damage your computer and infect others too.

Ugly E-Mail & Schemes to Get Your \$

Do not reply to junk e-mail ! Delete it!

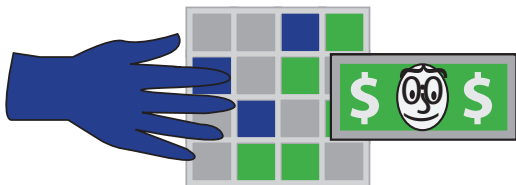
Be very careful about opening e-mail or clicking on links sent from anyone you don't know and trust.

"Spam" is junk e-mail that you never asked for. Spammers send out millions of advertising and often offensive material in hopes someone will respond. Don't answer, just delete it.

"Phishing" is an online scam that uses spam or pop-up messages to trick you into sharing personal information like your Social Security number or passwords. Phishers disguise their e-mails and web sites as banks or other trusted institutions. They try to trick you into giving them your account numbers and passwords so they can steal your identity, drain your bank account or run up credit card bills.

Protect yourself. Do not reply or click on links in any e-mail or pop-up that asks for personal information, especially if it is in response to an unsolicited e-mail.

If you want to use an online account, type the Web address directly into your Internet browser, don't click on an e-mail link. Filters can greatly reduce spam, but they don't eliminate it.



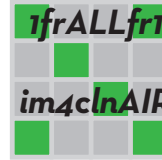
TAKING ACTION

There are things you can do right away that won't take a lot of time or cost a lot of money. Some just require a change of habit.

Passwords

Passwords protect the data you keep on your computer, including private accounts, documents and access to identifying information.. Passwords are the keys to your electronic house.

The best way to keep computer invaders ("hackers") and others from figuring out your password is to try to use a combination of 8-15 capital and lower case letters, as well as numbers and non-alpha-numeric characters, such as !,@,#,\$,%.

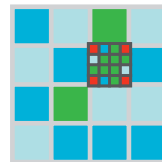


To help remember a more complex password, use a "passphrase." Think of a short saying, or a few words from a favorite poem that you'll remember, and turn it into a password by using numbers that sound like some of the letters in the phrase. For example, "I hate to be late" becomes the strong password "lh82bL8."

Most importantly, never share your password with anybody. Keep a record of passwords in a safe place and change them on a regular basis.

Patches & Updates

A patch or update is a small computer program that corrects known software problems. Software companies issue new, needed patches often and notify you of needed updates via the web or by e-mail if you have registered your product.

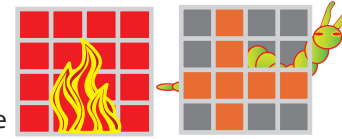


It's important to keep installing the latest patches. You can set your computer to do this automatically. It will check with software companies for patches to correct your operating systems, Internet Explorer and your anti-virus application.

Firewalls & Virus/Spyware Protection Software

Firewalls are filtering systems which restrict the movement of information between networked computer systems. They prevent private information from leaking out and keep unwanted programs from coming in.

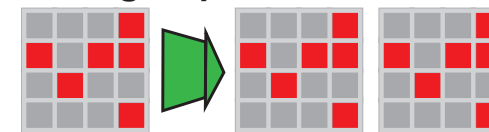
Virus protection software, or anti-virus software, attempts to identify, neutralize or eliminate malicious software. These programs will either try to "clean" or "disinfect" the virus, "quarantine" it, or "destroy" it, by scanning your computer on a regular basis and comparing it to a known list of malicious programs.



Relatively inexpensive and easy to use firewalls and anti-virus programs available that you can install on your PC. You can find information about them online by searching for "software firewall" or "anti-virus programs."

In your web browser settings, you can also increase security settings and block pop-up ads.

Making Copies



Regularly making copies of essential folders, files or documents from your computer is as important as having extra copies of your birth certificate or Social Security card. You can protect your documents and files by saving them on a disk, USB thumb flash drive or other storage hardware.

A Checklist

Here is a checklist of actions home users can take to protect their computer systems. It comes from the Computer Emergency Readiness Team (CERT) Coordination Center. More details on each item in this list are available at: www.cert.org/tech_tips/home_networks.html

- ✓ **Consult your system support personnel if you work from home.**
- ✓ **Use virus protection software.**
- ✓ **Use a firewall.**
- ✓ **Don't open unknown e-mail attachments.**
- ✓ **Don't run programs of unknown origin.**
- ✓ **Disable hidden filename extensions.**
- ✓ **Keep all applications (including your operating system) patched.**
- ✓ **Turn off your computer or disconnect from the network when not in use.**

Also, visit Seattle's information security website for more information.

See: www.seattle.gov/informationsecurity/