

BASIC COMPUTER SECURITY

GRAFTON-MIDVIEW PUBLIC LIBRARY

Inside this Handout

- 1 Computer Security
- 2 Malicious Software
- 3-4 Security Components
- 5 Email Threats & Spam
- 6 Phishing
- 7 General Precautions
- 8 Security Software

Why is Security Important?

Computer security is the process of preventing or detecting unauthorized use of your computer.

Malicious software on your computer can damage files, steal personal information and ultimately render your computer inoperable. Using the proper security can help prevent these types of problems.

Privacy Issues

Computers are used for everything from banking to shopping to communication, all things that you may not want strangers accessing. Generally when people use the Internet their activities are not private anymore. Anytime you apply for an account, register for something or purchase something online that information is saved. This information can be sold to marketing companies without your knowledge or consent. This can be either legal, or illegal, depending on the circumstances.

Things like online banking and shopping are usually done through secured websites which protect the user from identity theft, but no security is fool-proof and you should be aware of where you put personal information when you are on the Internet. Social networking sites are common places that private information is revealed if you are not careful.



Make sure your information is as secure as possible.

What is Malicious Software?

Malicious software, or malware, comes in several varieties and your security needs to be able to handle all of them. Malware is simply software that is designed to harm your computer in some way or access your computer without authorization.

- Viruses – A small piece of software that is designed to harm a computer. It attaches to legitimate software or files and each time the software is run or the file is accessed the virus activates and spreads as well.
- Worms – A worm is a small piece of software that uses computer networks and security holes to replicate itself.
- Trojans – A program that claims to be one thing but actually does something else and harms your computer or allows “back-door” access to your computer without your knowledge.
- Ransomware – Really a type of trojan which has become much more common. A very convincing pop-up will appear claiming to be a way to clean or secure your computer. They will claim they “found” threats on your computer. These are fake and will actually damage and lock the files and programs on your computer until you pay them money. Close these pop-ups using ALT + F4 or right-clicking the tab on the taskbar and selecting Close.



Example of ransomware pop-up

- Spyware/Adware – These are strictly for-profit malware that monitor web browsing, display unsolicited advertisements and redirect affiliate marketing revenue to the spyware creator. They do not spread like viruses and are installed by trojans or by exploiting browser security holes.

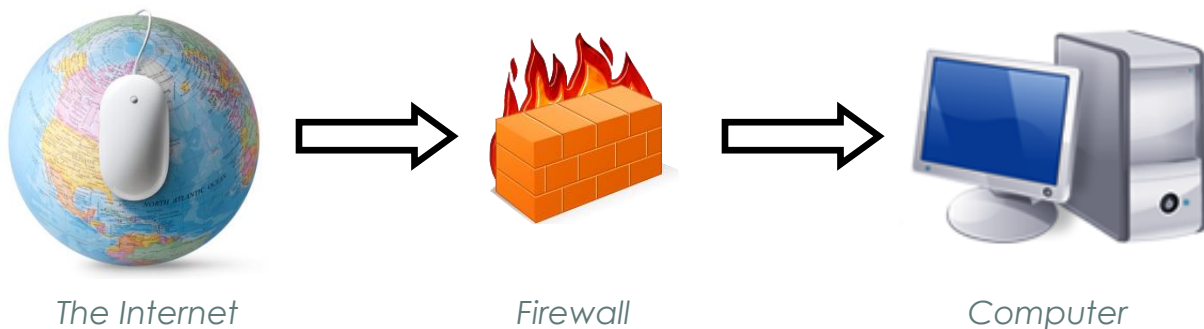
How to Protect Your PC

There are four basic components to a security system on a PC.

1. Firewall
2. Antivirus Software
3. Antispyware Software
4. Operating System Updates

Firewall

Firewalls block unauthorized entry into a network or a computer connected to the Internet. If a request, or data, does not pass the firewall's inspection it cannot go any further. Firewalls can be software-based, hardware-based, or both. If you have Microsoft Windows it has a built-in Windows Firewall already and many modems and routers have firewalls as well.



Antivirus Software

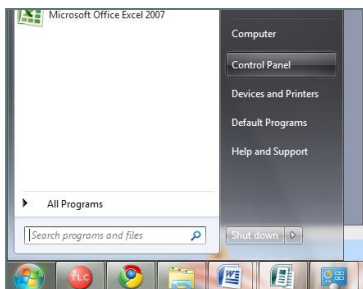
This software is necessary to secure your computer against threats from viruses, worms and trojans. Most new computers come with an antivirus package preinstalled, but it up to you to renew the subscription or replace the software before the trial period ends. Antivirus software is available in subscription and free variations, with many products having a basic free version and a subscription version. Whatever antivirus software you have installed should be updated and scanning your computer regularly. Check out product reviews and security information at CNET, an online computing magazine. <http://www.cnet.com/internet-security/>

Antispyware Software

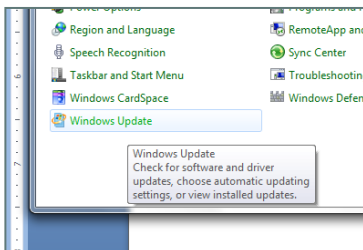
Spyware can result in data corruption, pop-up ads, hacker attacks and identity thefts so it is important to have software on your computer that can detect and delete spyware. This software can be part of antivirus software or purchased separately. Antispyware can also be downloaded for free just like antivirus software. Look for reviews at the same website listed on the previous page.

Installing Updates

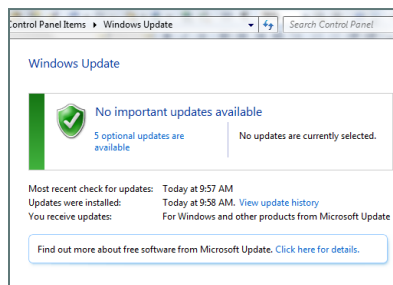
Some viruses and worms exploit a hole in an Operating System's security that has already been patched. If you do not install the updates with the patch then your computer could be susceptible to a virus that should not be a threat. This does not just apply to the Operating System, but all security software on your computer. Keep things up-to-date for optimal performance. Check for Windows updates by doing the following (Windows 7):



1. Open the CONTROL PANEL from the Start Menu.



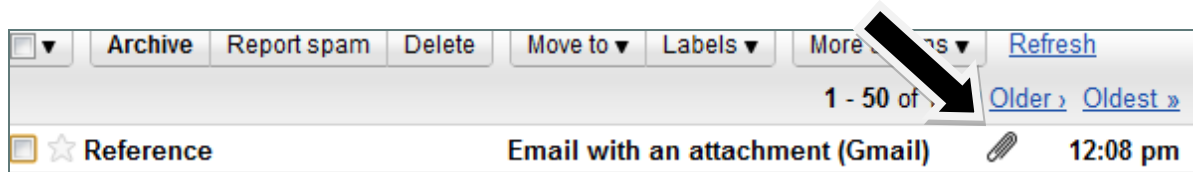
2. Click on WINDOWS UPDATE.



3. Install IMPORTANT updates and OPTIONAL updates.

Email Threats

Viruses in emails usually come through attachments. These are files that are attached to an email message like images or documents. You can tell when a message has an attachment because the message will have a paperclip icon. Do not open attachments from unknown senders and delete the message immediately.



When you get an email from someone you know with an attachment then you should pay attention to the type of file you have received.

Normally if you have an updated antivirus program it will warn you when you try to open an infected file so you shouldn't have to worry about email attachments from known senders.

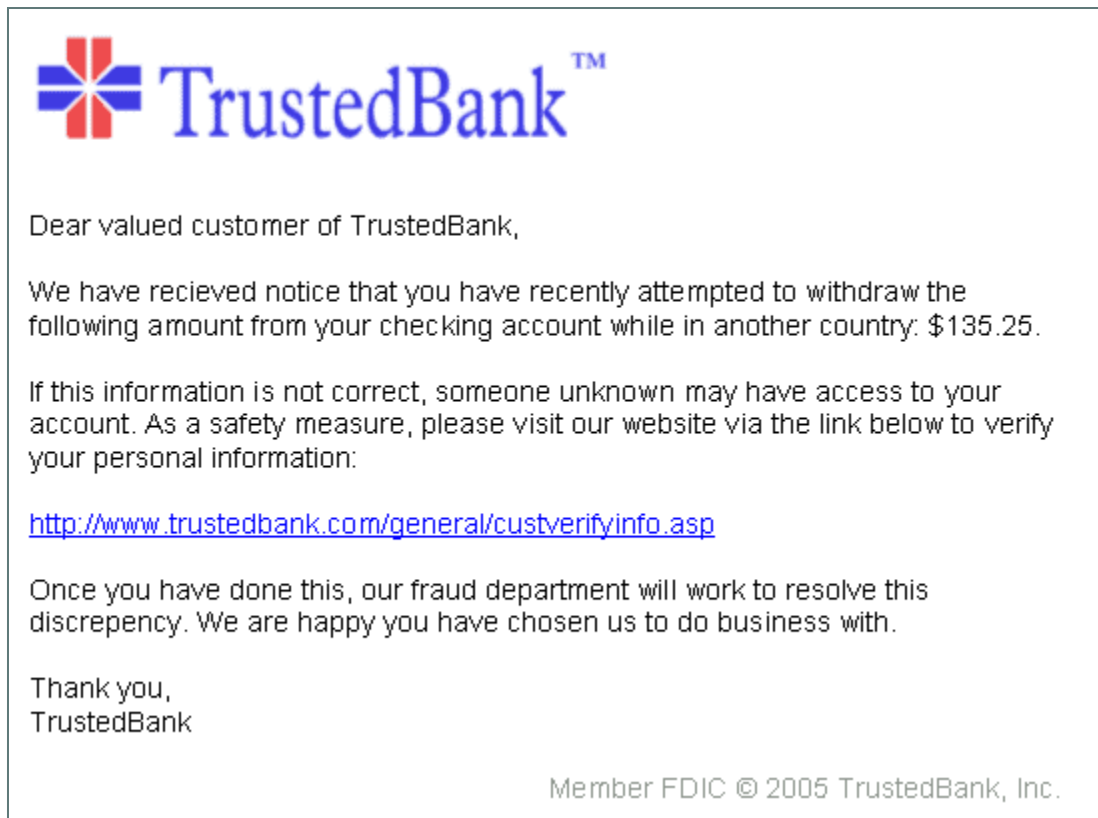


- Graphics, photos, animations, images (.gif, .jpeg, .mpeg, .tiff, .png, .jpg, .bmp)
- Audio, movie (.ram, .mp3, .mp4, .wma)
- Spreadsheet (.xls, .xlsx)
- Database (.mdb)
- Text document (.txt, .doc, .rtf, .wps, .wks, .docx, .pdf)
- PowerPoint presentation (.ppt, .pptx, .pps)
- Program (.exe, .zip, .vbs)

Viruses usually come in **.exe** (Executable) or **.vbs** (Visual Basic Scripting) format. **.jpg** (Images) may also have a virus embedded, although that is rarer. A **.zip** is just a zipped folder used to compress large files. Files inside can be anything, including viruses. All four of these files may *sometimes* be viruses and *sometimes* be safe files.

Phishing

This is a method of online identity theft but “phishers” can also infect computers with viruses and other malicious software. Phishing is mostly associated with email messages from banks, credit card companies and other commercial businesses. These messages look authentic and attempt to get victims to reveal personal information that can be used for identity theft.



Example of what a phishing email might look like from a bank.

If you are not sure about an email then move your mouse over the link but do not click on it. When the mouse is on the link itself your browser will display the actual address (URL) at the bottom of the screen. You can then check to see if the link matches.



You should never give out personal information or account information from an email link. Go directly to your bank's website instead which will be secure.

Security Precautions

1. Don't run any programs of unknown origin.

Never run/install a program that is not authorized by a company or person that you trust. Windows 7 will usually ask you to confirm any installation before proceeding, especially if Windows does not recognize the author of the program. Programs can contain viruses that will infect a computer.

2. Turn off your computer or unplug the network cable when not in use.

Your computer cannot be attacked when it is off or not connected to the Internet. Rebooting is a good idea for maintenance reasons as well.

3. Keep your private information private.

Be careful who you give your information to and never give it out unless you are certain of who will be reading it. Check your browser for the lock symbol in the address bar at the top or the status bar at the bottom. This means that the website is secure. Also, if you see *https://* in the front of the web address it means the website is using Secure Sockets Layer (SSL) technology that encrypts data and requires a code.

4. Research suspicious information.

If you see something suspicious do some research online to find out if something is legitimate and not a hoax of some sort.

5. Baits

Do not take offers of free products or services at face value. These are likely intended to fool you into downloading infected files or will infect your computer when you click on them. Also be wary of any messages that ask you to "validate" information, these are often phishing attempts.

Security Software

Go to these links for security software, virus lists, security hoaxes and current threats. This list is not comprehensive.

Norton Antivirus (Symantec)

<http://antivirus.norton.com>

McAfee Antivirus

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

Kaspersky Antivirus

<http://usa.kaspersky.com/>

Panda Security Software

<http://www.pandasecurity.com/usa/>

Cnet.com Security Software Center

<http://download.cnet.com/windows/security-software>

Wikipedia (variety of security related entries)

<http://en.wikipedia.org/wiki/Antivirus>

Hoaxbusters

<http://www.hoaxbusters.org/>

Revised 11/10 FB



Grafton-Midview Public Library

983 Main Street

Grafton, OH 44044-1492

Tel: 440-926-3317

Fax: 440-926-3000

Web: www.graftonpl.lib.oh.us