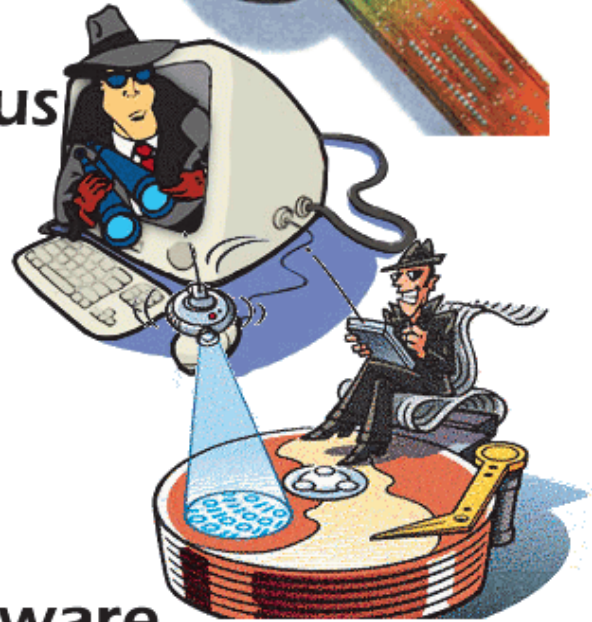




Computer Maintenance



Anti-virus



Anti-Spyware



Indian and Northern
Affairs Canada

Affaires indiennes
et du Nord Canada

Purpose of this IT Computer Security Guide



Most computers that go in for servicing have various problems; pop-ups and slow computer response are the most common of those problems. A computer that has these problems can be fixed very easily. Windows has various programs that you can use to scan and optimize a computer. In this guide we will be taking a look at those utilities as well as utilizing some free software utilities available on the Internet.



Disclaimer: Please note that this is meant to **be a guide and not a solution to all your computer maintenance and troubleshooting needs**. KAIT/KCDC are in no way responsible for any loss or corruption of data or the loss of use of the computer system due to complications caused by the software used in this guide. The steps used in removing and preventing spyware and viruses are merely suggestions to be taken at the discretion of the person(s) using this guide.

It is very important to note that you should **backup** crucial data (like documents and pictures, etc.) before attempting to clean out viruses or spyware from your computer in the event that any scans or virus removals render the system inoperable. This downtime may be temporary until you can get the system operational again and it may provide useful to have a backup copy of important documents in case you need to setup the user on a temporary workstation. Also ensure that you have all your original disks that came with the computer in the event that you may need them to do a restore. There are some cases where a computer is too far breached in security that the only way to make it completely operational again is to do a complete restore. This is what is referred to as a 'destructive restore' because it needs to wipe your hard-drive and do a factory re-install of the operating system and applications.

**NOTE:**

Some resources that **compliment this security guide** can be found on our website at <http://www.kait.ca> . Click on the IT Security course and login using the username: **itsecurity** and the password: **itsecurity** . You will be able to access the Worksheets, PowerPoint Lecture Slides and Jeopardy Game and IT Security Activities. You will also be able to download the IT Security Quiz to test the knowledge of those who have gone through this IT Security Guide.



IT Security Kit Contents

- KAIT: IT Computer Security Guide
- DVD Tutorials Videos on Malwarebytes, Spybot: S&D (Search and Destroy), Avast, Task Manager/Process Explorer
- Worksheets
- IT Security Quiz
- PowerPoint Lecture Presentation (available at www.kait.ca)
- Jeopardy IT Security Game (using PowerPoint) (available at www.kait.ca)

If you have any suggestions to make this guide better or if you require clarification on some points in this guide, we are open to suggestions. We are not, however, available to do e-mail consultations on fixing your computer. Please consult your local PC Repair Depot for computer advice and possible PC Repair needs.



KAIT
Box 489
Air Ronge, SK
S0J 3G0

E-mail us at: kait@kait.ca or visit our website <http://www.kait.ca>

Thanks,

Nick Daigneault
KAIT, IT Training Manager



NOTE: You will see important notes like these spread throughout this guide. Pay close attention to them.



NOTE: This overview is for PCs with the Windows Vista operating system on them, the steps may differ on other Windows operating systems.

IMPORTANT: Before running any spy-ware or virus programs it is advised that you turn off system restore.

Why is Security Important?



Computer and network security help to keep data and equipment functioning and provide access only to appropriate people. Everyone in an organization should give high priority to security because everyone can be affected by a lapse in security.

Theft, loss, network intrusion, and physical damage are some of the ways a network or computer can be harmed. Damage or loss of equipment can mean a loss of productivity. Repairing and replacing equipment can cost the company time and money. Unauthorized use of a network

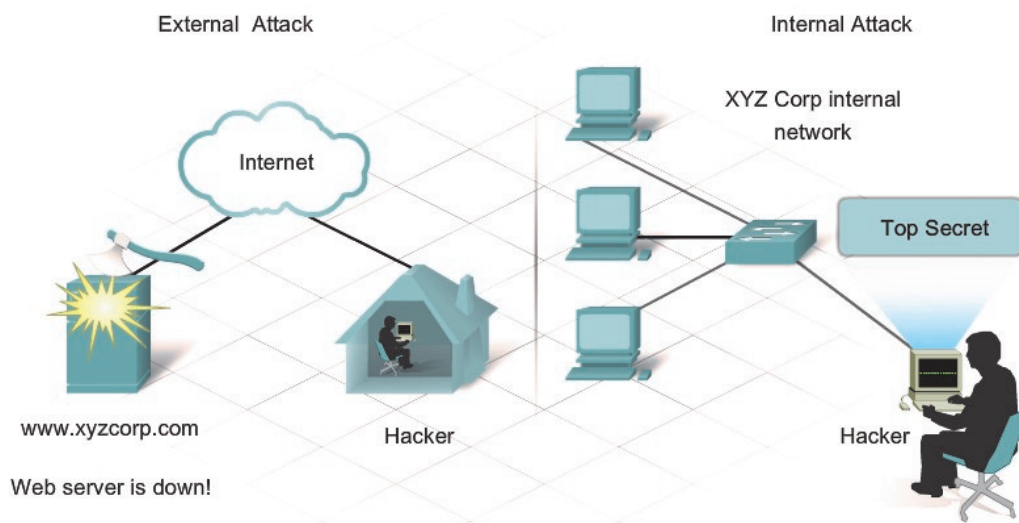
can expose confidential information and reduce network resources.

An attack that intentionally degrades the performance of a computer or network can also harm the production of an organization. Poorly implemented security measures to wireless network devices demonstrate that physical connectivity is not necessary for unauthorized access by intruders.

Maintaining good security practices with computer equipment is a must to ensure the constant safety of data and network integrity and for our own personal safety. Just to clarify the extent of damage and identity theft that can take place on a single computer, think of a person gaining full access to your computer because you or another individual inadvertently downloaded a virus or some spyware software to your computer. Now that they have access they can steal your files, run programs, log your keystrokes and gain access to your account names and passwords, credit card information and more. They may also turn your computer into a 'zombie' (a term you'll learn more about later) that allows the individual who compromised your computer's security to utilize it in internet attacks without you even knowing.

Unless you educate and properly train yourself in preventing this, plugging yourself into a network or the internet can be quite risky. This guide is not meant to frighten you from connecting to a network or the internet, but to educate you.

What types of security threats are there?



To successfully protect computers and the network, computer users must understand both types of threats to computer security:

Physical - Events or attacks that steal, damage, or destroy equipment, such as servers, switches, and wiring.

Ex. Theft of laptop with confidential data, arson attack on server room

Data - Events or attacks that remove, corrupt, deny access, allow access, or steal information.

Ex. Virus/Worm/Trojan Attacks, Spam, Cracking your network security

Security threats from network intruders can come from both **internal** and **external** sources.

External Threats

External threats arise from individuals working outside of an organization. They do not have authorized access to the computer systems or network. External attackers work their way into a network mainly from the Internet, wireless links or dialup access servers.

- Unstructured – Attackers use available resources, such as passwords or scripts, to gain access and run programs designed to vandalize
- Structured – Attackers use code to access operating systems and software

What types of security threats are there?

Internal Threats—We are our own worst enemy

Internal threats occur when someone has authorized access to the network through a user account or have physical access to the network equipment. The internal attacker knows the internal politics and people. They often know what information is both valuable and vulnerable and how to get to it.

However, not all internal attacks are intentional. In some cases, an internal threat can come from a trustworthy employee who picks up a virus or security threat, while outside the company and unknowingly brings it into the internal network. For this reason alone, all computers that have been exposed to 'outside' networks (internet in hotel rooms, at home, etc.) should be subject to scans prior to reintegration into the regular network. Bringing in a virus or security threat (spyware) from the outside would completely bypass any security put in place to prevent such 'external'-type attacks, kind of like a Trojan horse.



Most companies spend considerable resources defending against external attacks however most threats are from internal sources. According to the FBI, internal access and misuse of computers systems account for approximately 70% of reported incidents of security breaches.

To help curb theft within any school or organization, it is always recommended that valuable items should be locked up in a secure location where only a limited amount of people have access. Also, if an individual requires access to the hardware, they should sign it out and be aware that they are responsible in full for that piece of hardware should it go missing.

Virus, Worm, Trojan—What's the difference?



A **virus** is a program written with malicious intent and sent out by attackers. The virus is transferred to another computer through e-mail, downloaded files, file transfers, instant messaging, web applications and social networking sites. The virus hides by attaching itself to a file on the computer. When the file is accessed, the virus executes and infects the computer. A virus has the potential to corrupt or even delete files on your computer, use your e-mail to spread itself to other computers, or even erase your entire hard drive. Computer users should know that viruses do not start by themselves, they need to be activated. This means that you have to willingly click on an infected file to activate it, or click on a URL (link) that will take you to a website that will exploit the vulnerabilities of your web browser to execute the virus. If the virus is spread to other computers, those computers could continue to spread the virus.



Some viruses can be exceptionally dangerous. The most damaging type of virus is used to record keystrokes, called a **keylogger**. These viruses can be used by attackers to harvest sensitive information, such as passwords and credit card numbers. Viruses may even alter or destroy information on a computer. Stealth viruses can infect a computer and lay dormant until summoned by the attacker.



A **worm** is a self-replicating program that is harmful to networks. A worm uses the network to duplicate its code to the hosts on a network, often without any user intervention. It is different from a virus because a worm does not need to attach to a program to infect a host. Worms most commonly infect systems because of security flaws in operating systems. The best way a computer user can protect themselves from these types of infections is to ensure their operating system and other commonly used programs are up to date with security and software patches. Even if the worm does not damage data or applications on the hosts it infects, it is harmful to networks because it consumes bandwidth. In worse case scenarios it could completely halt network activity including traffic in and out to the internet.



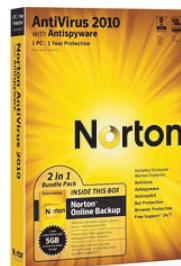
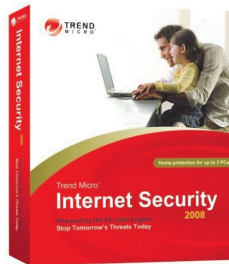
A **Trojan** is technically a worm, and like a worm the Trojan does not need to be attached to other software. Instead, a Trojan threat is hidden in software that appears to do one thing, yet behind the scenes it does another. Trojans are often disguised as useful software. The Trojan program can reproduce like a virus and spread to other computers. Computer data damage and production loss could be significant. A technician may be needed to perform the repairs, and employees may lose or have to replace data.

Virus, Worm, Trojan—What's the difference?

An infected computer could be sending critical data to competitors, while at the same time infecting other computers on the network. In some cases, Trojans can be designed intelligently to fool computer users into believing they are using a legitimate program like an anti-virus or anti-spyware program, but once they close the software it will execute its payload and possibly cause damage to the user's computer system. This is also a good reason to only download from trusted sources and not download just any anti-virus or anti-spyware software.



Virus protection software, known as anti-virus software, is software designed specifically to detect, disable, and remove viruses, worms, and Trojans before and after they infect a computer. Anti-virus software becomes outdated quickly, however, and it is the responsibility of the computer user to apply the most recent updates, patches, and virus definitions as part of a regular maintenance schedule.



Usage of the anti-virus software will be discussed later in this guide. Some examples or trusted free antivirus software include:

- **Trend Micro Housecall Online Virus Scan**
<http://housecall.trendmicro.com>
- **AVG Anti-Virus**
<http://free.avg.com>
- **Avast! Anti-Virus**
<http://www.avast.com/en-ca/free-antivirus-download>

How is web security important?

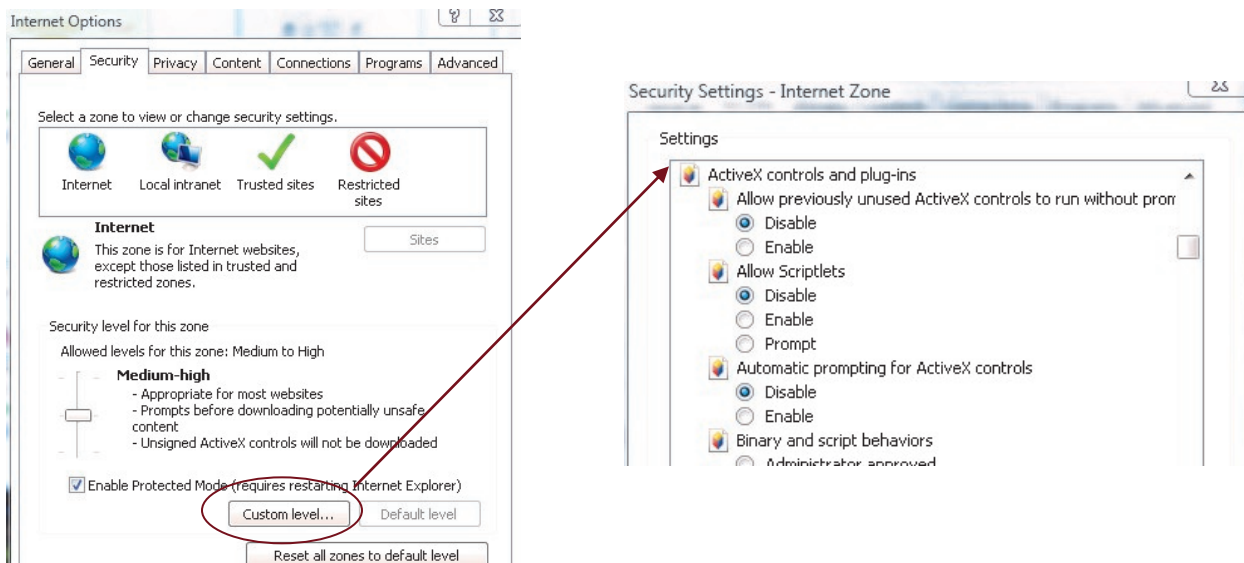


Web security is important because so many people visit the World Wide Web every day. Some of the features that make the web useful and entertaining can also make it harmful to a computer.

Tools that are used to make web pages more powerful and versatile, can also make computers more vulnerable to attacks. These are some examples of web tools:

- **ActiveX** – Technology created by Microsoft to control interactivity on web pages. If ActiveX is on a page, an applet or small program has to be downloaded to gain access to the full functionality. This only applies to Internet Explorer browsers.
- **Java** – Programming language that allows applets to run within a web browser. Examples of applets include a calculator or a counter. This can be used on any web browser such as Opera, Firefox, or Internet Explorer.
- **JavaScript** – Programming language developed to interact with HTML source code to allow interactive websites. Examples include a rotating banner or a popup window. Javascript is not to be confused with ‘Java’ as the two are completely unrelated. Javascript can be run in any browser that allows it.

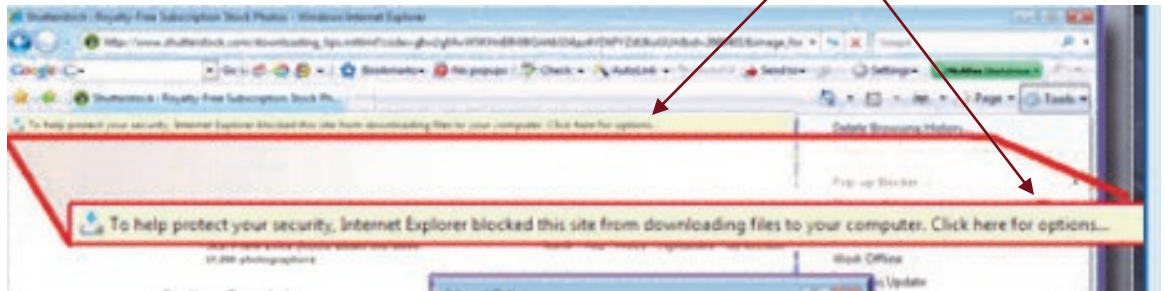
Attackers may use any of these tools to install a program on a computer. To prevent against these attacks, most browsers have settings that force the computer user to authorize the downloading or use of ActiveX, Java, or JavaScript, as shown below.



To access these security settings in Internet Explorer, click on **Tools** then “**Internet Options**”

How is web security important?

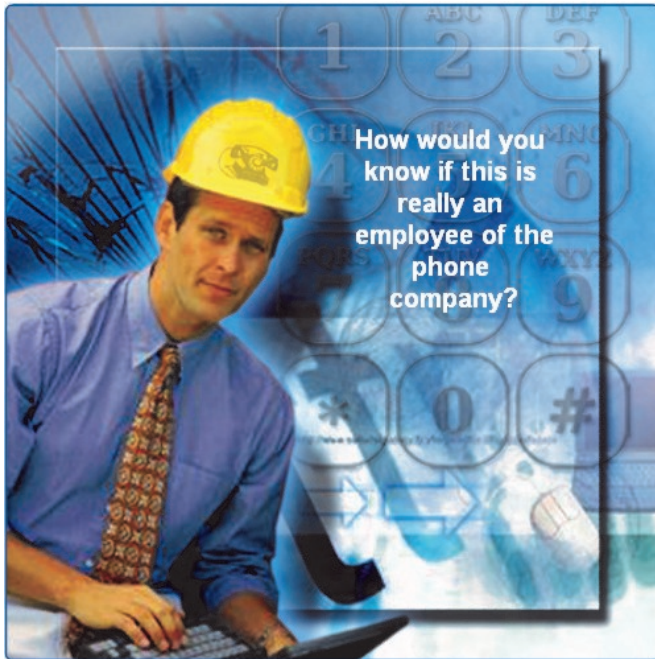
Since the release of Windows XP Service Pack 2 and the newer version of Internet Explorer, you now get security dialog boxes popping up prompting for your permission to install certain programs directly from the web. This includes programs like Adobe Acrobat Reader, Adobe Flash Player, Windows Media Extension, etc. Some prompts appear in the form of an Internet Security Bar (yellow stripe just below your address bar or tabs) or an in-your-face dialog box (bottom image).



These security warning dialog boxes can be very useful in thwarting web-attacks as sometimes merely clicking a link will take you to a website that will automatically install software without your knowledge. With these new security features in place, this will only happen if your web-security is disabled, or if your operating system and/or Internet browser has a security flaw; in which case you should be sure to avoid this by updating your security and software patches regularly.



Social Engineering? Is that a new University Degree?




Social engineering is a term that refers to the ability of something or someone to influence the behaviour of a group of people. In the context of computer and network security Social Engineering refers to a collection of techniques used to deceive internal users into performing specific actions or revealing confidential information.


With these techniques, the attacker takes advantage of unsuspecting legitimate users to gain access to internal resources and private information, such as bank account numbers or passwords.

Social engineering attacks exploit the fact that **users are generally considered one of the weakest links in security (what? It's true!)**. Social engineers can be internal or external to the organization, but most often do not come face-to-face with their victims.

Three of the most commonly used techniques in social engineering are: **pretexting, phishing, and vishing.**



Pretexting is a form of social engineering where an invented scenario (the pretext) is used on a victim in order to get the victim to release information or perform an action. The target is typically contacted over the telephone. For pretexting to be effective, the attacker must be able to establish legitimacy with the intended target, or victim. This often requires some prior knowledge or research on the part of the attacker. For example, if an attacker knows the target's social security number, they may use that information to gain the trust of their target. The target is then more likely to release further information.



Phishing is a form of social engineering where the phisher pretends to represent a legitimate outside organization. They typically contact the target individual (the phishee) via email. The phisher may ask for verification of information, such as passwords or usernames in order prevent some terrible consequence from occurring. (Ex. Cancelling your bank account if you don't respond to the e-mail or asking you to visit a bogus website to submit your confidential information).

Social Engineering? Is that a new University Degree?



Vishing / Phone Phishing: A new form of social engineering that uses Voice over IP (VoIP) is known as vishing. With vishing, an unsuspecting user is sent a voice mail instructing them to call a number which appears to be a legitimate telephone-banking service. The call is then intercepted by a thief. Bank account numbers or passwords entered over the phone for verification are then stolen.



NOTE: There is rarely a need to give out sensitive personal or financial information online. Be suspicious. Use the postal service to share sensitive information..

In addition to social engineering, viruses, worms and Trojan horses can be used in conjunction to obtain information from users. Users may be tricked into clicking a link to a website that will exploit an operating system vulnerability and allow a virus to be installed on the system. This virus may log personal information on the computer without the knowledge of the user(s) and submit it to the creator of the virus.

Here are some basic precautions to help protect against social engineering:



- Never give out your password
- Always ask for the ID of unknown persons
- Restrict access of unexpected visitors
- Escort all visitors
- Never post your password in your work area
- Lock your computer when you leave your desk
- Banks and other sites that do financial transactions would never e-mail you requesting personal information; visit their regular website by typing in the URL of the website yourself in a browser address bar. Never click a link to a financial institution or business in an e-mail as it may be a fraudulent redirector link that will take you to a website that looks similar to the actual site.
- With the popularity of social networking sites such as Facebook, you should be cautious about installing 'applications' to your profile without knowing what they may do or what you may allow it to have access to on your profile and computer. Also, just like e-mail, do not completely trust links sent to you just because it appears to come from a friend.

Adware, Spyware, Grayware..... Tupperware?



Adware, spyware, and grayware are usually installed on a computer without the knowledge of the user. These programs collect information stored on the computer, change the computer configuration, or open extra windows on the computer without the user's consent.

Adware is a software program that displays advertising on your computer. Adware is usually distributed with downloaded software. Most often, adware is displayed in a popup window. Adware popup windows are sometimes difficult to control and will open new windows faster than users can close them. This could become an annoyance to the user and could potentially cause the system to use up all its resources, ultimately slowing down the computer and causing it to crash often.

This type of software, sometimes called **Shareware**, is usually legal and 'bundled' with free-software downloads such as free online game websites and free programs & utility websites (like free antivirus, free music download, etc.) Read the terms of the free software download to be sure it does not come bundled with any additional software. This type of software may be difficult to remove and it may cause some other software to become disabled.

Grayware or **malware** is a file or program other than a virus that is potentially harmful. Many grayware attacks are phishing attacks that try to persuade the reader to unknowingly provide attackers with access to personal information. As you fill out an online form, the data is sent to the attacker. Grayware can be removed using spyware and adware removal tools.

Spyware, a type of grayware, is similar to adware. It is distributed without any user intervention or knowledge. Once installed, the spyware monitors activity on the computer. The spyware then sends this information to the organization responsible for launching the spyware.

Tracking Cookies are a form of spyware but are not always bad. They are used to record information about an Internet user when they visit websites. Cookies may be useful or desirable by allowing personalization and other time saving techniques. Many web sites require that cookies be enabled in order to allow the user to connect. Cookies that are installed by spyware and are more invasive may be referred to as Super Cookies or Data Miners. These types of cookies are generally removed by spyware scanners. It is still good practice to **delete your cookies** once in awhile from your internet browser. This will cause some sites to lose your personal preferences (such as news websites), but you can easily set them again.



Spam? It's not what's for dinner?



Not this spam!

Spam, also known as junk mail, is unsolicited e-mail. In most cases, spam is used as a method of advertising; however, spam can be used to send harmful links or deceptive content. Spam is a serious network threat that can overload ISPs, email servers and individual end-user systems. A person or organization responsible for sending spam is called a **spammer**.

Spammers often make use of unsecured email servers to forward email. Spammers can use hacking techniques, such as viruses, worms and Trojan horses to take control of home computers. These computers are then used to send spam without the owner's knowledge. Spam can be sent via email or more recently via Instant messaging software.

It is estimated that every user on the Internet receives over 3,000 spam emails in a year. Spam consumes large amounts of Internet bandwidth and is a serious enough problem that many countries now have laws governing spam use.



When used as an attack method, spam may include links to an infected website or an attachment that could infect a computer. These links or attachments may result in lots of windows designed to capture your attention and lead you to advertising sites. These windows are called **popups**. Uncontrolled popup windows can quickly cover the user's screen and prevent any work from getting done (as shown in the graphic to the left).

Many anti-virus and e-mail software programs automatically detect and remove spam from an e-mail inbox. Some spam may still get through, so look for some of the more common indications:

- * No subject line
- * Incomplete return addresses
- * Computer generated e-mails
- * Return e-mails not sent by the user

If I eat too much spam, will it cause me to spoof?

Popups and **pop-unders** are additional advertising windows that display when visiting a web site. Unlike Adware, popups and pop-unders are not intended to collect information about the user and are typically associated only with the web-site being visited.

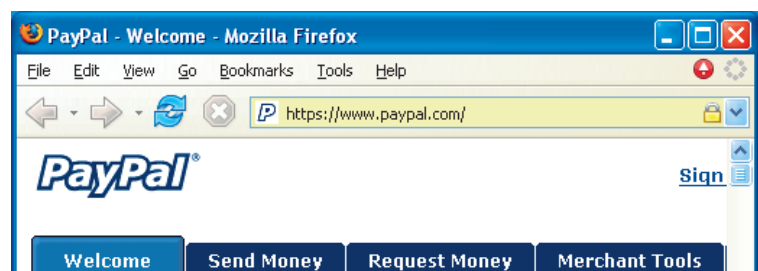
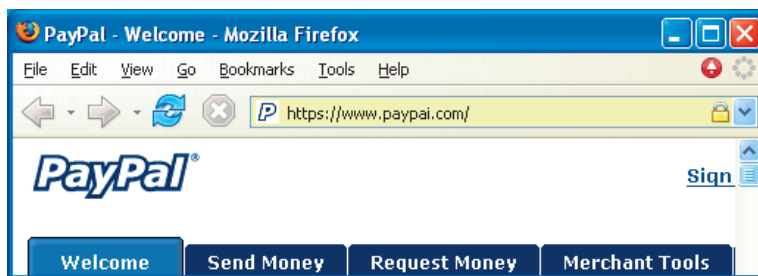
- Popups: open in front of the current browser window.
- Pop-unders: open behind the current browser window.

With things like **popups** and **pop-unders** infiltrating your system, it becomes hard to differentiate legit windows from spam windows. This also becomes a form of social engineering attack when have become caught in the chaos and a popup window that looks like a computer explorer window (to browse your files) or a 'Click this button to close this window' graphic tricks you into clicking it. This deception is often referred to as **spoofing** when it mimics something else.

You may receive **spam e-mails** that look like they are coming from your bank, Paypal, Facebook, or some other form of legitimate internet service. More than likely this e-mail is a spoofed e-mail that can be discarded as spam. As mentioned before, you may also receive an e-mail message or instant message from what appears to be one of your 'friends.' This e-mail or instant message will entice you to click a link or open an attachment with the guise that it is 'safe' because it comes from a friend. Often it may be just because a virus or spyware has obtained enough information from an infected computer that is harvested the individual's address book and can now **spoof** that information. If you are unsure if the attachment is actually coming from a trusted source, it may be a better idea to not open it.

Example:

One of these websites is **spoofed** (fake). If you weren't paying close attention, you would see the top website is actually `paypai.com` and not `paypal.com`. They both look very similar. If you logged into the fake website, they would now have your personal login to PayPal.



The interwebs is attacking! What do I do?



Millions of computers are being infected with some form of virus or spyware on a daily basis. This is largely due to users who are unaware of the security dangers they put themselves into simply by browsing the internet or downloading programs from untrustworthy sources in order to gain access to something they want (ie—free music, games, programs, movies, etc.).


Viruses and **spyware** are now spreading even quicker with the popularity of social networking tools such as Facebook, Bebo, Hi5, MSN Messenger, Yahoo Messenger, AOL Instant Messenger, and the list goes on. These are not to say that these things are ‘bad’ and that we shouldn’t use them in order to protect our security. We should all be responsible computer users and take the time to educate ourselves on the potential security risks of using the tools to protect our own privacy and the privacy of others, especially when utilizing websites that contain our personal information.


We are probably going to encounter at least one form of virus or spyware in our lives. The question is, what do we do once we become infected? More importantly, how do we know if we’re infected or not?

Disable System Restore



The first thing we need to do is disable the operating system’s ‘**System Restore**.’ If your computer has become infected, viruses and spyware will plant itself in backup and restore files to keep your computer infected. If you clean your system and later do a roll-back or restore, it will re-infect your system from your backups. **For instructions on how to do this, refer to the DVD video on ‘How to Disable System Restore.’**

 **Reminder:** The steps used in the video are for Windows Vista. They are quite similar to Windows XP as the System Restore tab is usually found in the System’s Properties control panel.

 **Note:** It was said before, but at this stage it becomes very important to backup any essential data in the event that the virus and spyware removal have negative effects on your computer.

Once system restore is disabled, it will delete any ‘Restore Points’ that are in your computer. When the system is cleaned, you can reverse these steps to re-enable system restore and new clean restore points can be created.

MalwareBYTES (bites)... get it?

With System Restore disabled, we can now begin to scan our system for possible infections. If you don't already have security software installed, we can download free versions of trusted security software such as **Malwarebytes**.



Once you download, install, and update Malwarebytes you can use this security tool to scan your computer. **For instructions on how to download and install Malwarebytes, refer to the DVD video.** Whoah! Wait! Hold On! ... Don't scan the computer right away. Usually, we like to reboot the computer into '**Safe Mode**' first.

Booting Into Safe Mode

To boot into Safe Mode is a relatively easy step if you got rhythm. Tap, Tap, Tap, Tap-pity, Tap, Tap. Got it? Okay, great!

First step is to reboot your computer if it currently turned on. If it's not turned on then I guess the first step is to turn it on!



After a couple seconds after the computer starts-up or reboots, wait for the beep. After you hear the beep you can begin **tapping** the **F8** key located on the top row of keys on your keyboard.

If you are successful, you should see an Advanced Startup Menu screen with different options to boot your computer. Choose Safe Mode.

```
Windows Advanced Options Menu
Please select an option:

Safe Mode
Safe Mode with Networking
Safe Mode with Command Prompt

Enable Boot Logging
Enable VGA Mode
Last Known Good Configuration (your most recent settings that worked)
Directory Services Restore Mode (Windows domain controllers only)
Debugging Mode

Start Windows Normally
Reboot
Return to OS Choices Menu

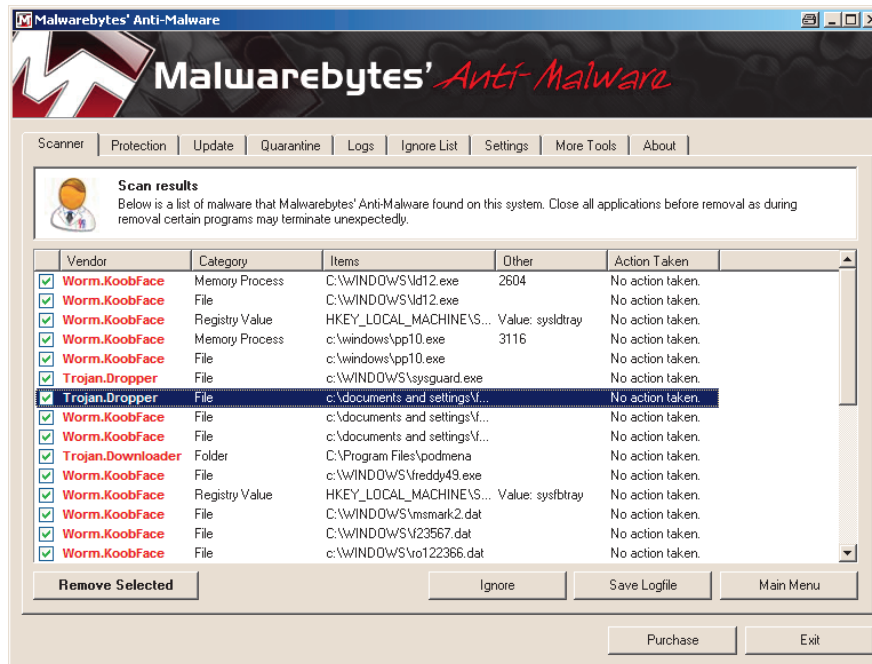
Use the up and down arrow keys to move the highlight to your choice.
```

Safe mode boots into an environment that only loads the basics in order to operate the system. It does not start up any extra programs or load any special drivers. This is a useful troubleshooting tool and an excellent tool for removing viruses and spyware.

Once in Safe Mode, you can start up Malwarebytes and begin a scan.

MalwareBYTES (bites)... get it?

Once the scan is complete, you may have to deal with the infections the program discovers.



Ensure that all the security threats Malwarebytes finds are selected (the green check marks on the left). Then click the “Remove Selected” button.

If you're a curious cat like I am, you'll want to take a look at what type of infections were discovered on your computer. **'Memory Process'** means it a file that was currently running in your system. **'Registry Value'** meant that it was registered in your System Registry as a program with libraries and everything else that's implied with that. **'File'** means that it was part of the program files or libraries required to run the actual program that was running in your computer system. What may also peak your curiosity is to see the locations of the actual files themselves. You can see that spyware will hide in a variety of places but mainly within the complex folder structure of your Windows folder.

At this time, it is recommended that you reboot the computer and let it boot normally. Once the computer is started up, open up Malwarebytes and run yet another scan to see if any infections have returned.



Persistent Spyware! What else can I do?

Very rarely is one program going to solve all your computer security needs. Malwarebytes should have handled most of the hard hitting spyware infections on your computer system, so why does it keep coming back? This is because each program uses its own unique approach to combating the infections. For this reason, using multiple programs to do security sweeps is recommended.

Spybot Search & Destroy



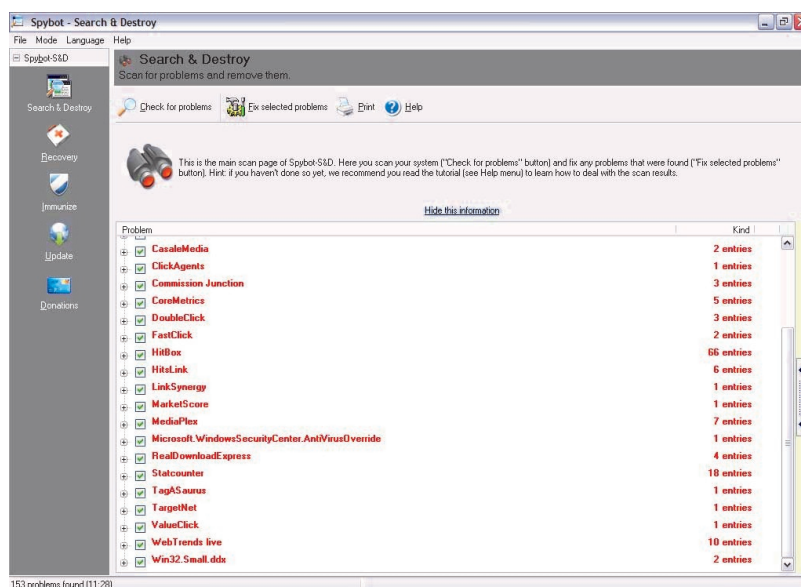
Once Malwarebytes has done all that it can do, you can utilize another program called Spybot Search & Destroy to do another scan on your system. **For instructions on how to download, install, and update Spybot Search & Destroy, please refer to the DVD Video.**



When installing Spybot Search & Destroy, ensure that you do not install TeaTimer or SDHelper with the program unless you plan on keeping this software installed once you're done scanning the system. These programs will run in the background to help prevent further infection, but be advised that they also use up system resources to protect your system. Once again, boot into Safe Mode and run the Spybot Software.

Once the Spybot scan is complete, it will list any system threats that are registered in its database (which is why it's important to update the software 'before' scanning). Ensure that all threats are selected (the green arrows on the left of the threat) and click "Fix Selected Problems."

Reboot and do this scan again while Windows is running normally.



Spyware Removed! What about the viruses?

These days it's kind of hard to differentiate from viruses and spyware, as both wreak havoc on your computer in a similar fashion. Running spyware scans won't necessarily remove viruses from your computer, although it may remove the occasional Trojan virus that is associated with a particular Spyware infection.



For this reason, we must also run Virus Scans to ensure that your system is free of infection. In this guide we will use the Avast! Virus scanner to scan your system. **For instructions on downloading, installing and updating Avast! Antivirus please refer to the DVD Videos.**



Until the Spyware scans, you will be unable to leave this scan unattended (well not for long anyway). When Avast! finds a virus, you will need to address it immediately. You will see a dialog box pop up similar to this one:



Take a careful look at the file it scanned and see if it's a file you need or recognize. If you are unsure, you can **“Move to Chest”** or if you want to remove the threat completely you can hit the **“Delete”** button.



Note: Also pay special attention to the part about scheduling a boot-time scan to remove any startup and boot sector viruses.

I want a second opinion. Is there a doctor in the house?

Just like the spyware scanning, one virus scanner is typically not enough to rely on to clean your computer system. Since you do not want to download and install yet another virus scanner (and it's not recommended anyway as having two virus scanners on your system will ultimately slow it down enormously), we will utilize an online scanner. This scanner will require some initial download, but it is temporary and relatively small in size.



The online virus scanner we are going to utilize here is called **Trend Micro Housecall**. It is a free online scanner that will scan your system from its web engine located on the Trend Micro website. **For instructions on how to access this online scanner and initialize the temporary download, please refer to the DVD.**



Let the scan finish and follow the easy to use 3 step Trend Micro Housecall wizard. This virus scanner will look similar to other virus scanners and any virus found will need to be addressed.

Whew! That was a close one. How do I prevent this from happening again?

Security measures can be put into place to help outright prevent or minimize the system infection should another one occur.

Anti-Virus

Anti-virus software can be used as both a preventative tool and a reactive tool. It will prevent further infection provided that your virus definitions are kept up to date and can also detect, and remove viruses, worms and Trojan horses. Antivirus software should be installed on all computers in any network. Although there are many anti-virus programs available, I am going to recommend that **Avira's Anti-Vir** program be downloaded and installed.



This program can be downloaded at <http://www.free-av.com>.



Note: Be sure to uninstall any virus scanners that were installed BEFORE installing this antivirus software.

The reason I recommend this product over others is mainly the fact that it's free and does not hassle you to re-download or register every month. You should only have to re-download if a new version is available.

Spyware Protection



As mentioned previously, **Spybot** has a **TeaTimer** and **SDHelper** program that will install onto your computer if you want to use it for long-term protection against spyware threats. The **TeaTimer** will monitor your system for any spyware signatures. The **SDHelper** will monitor your browser configuration settings and prevent programs from adjusting your homepage settings and from installing any unwanted 'Browser Helper Objects (BHOs)' which attempt to install search bars and super cookies and other undesirable programs.

Other than Spybot, most spyware removal programs require you to initiate the scan. In order to enjoy the benefits of real-time scanning you usually have to pay for this type of software.

Whew! That was a close one. How do I prevent this from happening again?

Software patches and updates

One of the most common methods that a hacker uses to gain access to hosts and/or networks is through software vulnerabilities. It is important to keep software applications up-to-date with the latest security patches and updates to help deter threats. A patch is a small piece of code that fixes a specific problem. An update, on the other hand, may include additional functionality to the software package as well as patches for specific issues.



Note: Keep in mind that any software you download, especially software that connects to the internet or your network, should be updated. You may need to visit the software vendor's website to obtain software updates or patches. For Operating System updates for the Windows OS, you can find the Automatic Updates configuration in the Control Panel.

OS (operating system, such as Linux, Windows, etc.) and application vendors continuously provide updates and security patches that can correct known vulnerabilities in the software. In addition, vendors often release collections of patches and updates called service packs. Fortunately, many operating systems offer an automatic update feature that allows OS and applications updates to be automatically downloaded and installed on a host.

Popup Blockers

Popup stopper software can be installed to prevent popups and pop-unders. **Many web browsers include a popup blocker feature by default.** Note that some programs and web pages create necessary and desirable popups. Most popup blockers offer an override feature for this purpose.

Be careful not to overload on pop-up blocker software as it may be difficult to track down why a website won't work properly if you have 2 or 3 different security programs preventing pop-ups when the website requires this.

Is it possible for 'me' to become an antivirus program?

Glad you asked! Of course it is. Using your new found knowledge and the tools that are freely available from your operating system and the internet, you can easily combat security threats on your own system.

Be suspicious of any activity that seems odd on your computer. Some of the signs that a virus, worm or Trojan may be present on your system include:

- Your computer starts acting abnormally
- A program does not respond to mouse and keystrokes
- Programs starting or shutting down on their own
- Email program begins sending out large quantities of email
- CPU usage is very high
- There are unidentifiable, or a large number of processes running
- Computer slows down significantly or crashes

Using the Task Manger and/or Process Explorer



So you're probably wondering 'How do I know if my CPU usage is high?', or 'What processes are running?'. While most of this would be common knowledge for a technician, it is not so much for the average household computer user. You can utilize your own **Task Manager** to see exactly what is running on your system, how much memory is being used, and how much CPU time is being taken up.

Sometimes when legitimate programs such as the Windows Automatic Update Manager are running in the background, you will hear your hard drive whirring, and buzzing and your computer seems to be running a bit slower. Often this type of stuff is **mistaken** for a virus or spyware threat in action. To determine if there is a real threat on your computer system, you can open up the Task Manager and see exactly what's going on. You may also decide to download the **Process Explorer** program to further investigate the processes on your system.



Please refer to the DVD video on Using the Task Manager and Process Explorer for more information.

Congratulations! You're all done! Or... are we?

Viruses and spyware are going to be around as long as computers are still running. New virus threats are constantly emerging and new ways to infect a computer with spyware are being developed. This means that the learner never stops for us. We will need to constantly educate ourselves on computer security. We will need to determine what the threats are and how to protect ourselves from them. The best way to do this is to find a good source on the internet for information on computer security and keep up to date as you would with a daily newspaper. There are a lot of good technical articles out there even if you aren't very tech savvy.



Here are a few good links to check out whenever you have free time:

PC Mag's Security Watch Articles

<http://blogs.pcmag.com/securitywatch/>

How Stuff Works: The Computer Security Channels

<http://computer.howstuffworks.com/security-channel.htm>

Snopes.com: Virus Hoaxes & Realities

<http://www.snopes.com/computer/virus/virus.asp>

PC World: Security

<http://www.pcworld.com/topics/security.html>

For an excellent site for security guides and to see if one of your processes is a virus, you can search at:

Norton (Symantec) Threat Explorer

http://www.symantec.com/norton/security_response/threatexplorer