



Safe and Secure Computing

KSC Seminar Presented By

Steve Courtney

Director KSC Computer Training Team

With support from the KSC Computer Training Team



Jan 20th, 2011



Seminar Topics



- **Downloading and applying updates to programs**
- **PC Firewalls & Securing DSL/Cable Modem/Routers**
- **Malware, Anti-virus & anti-spyware programs**
- **Phishing - what it means and how to avoid**
- **Keyloggers - protecting your personal information**
- **Web Browser Cookies & safe web surfing**
- **Handling Spam emails**
- **Password selection and management**
- **Top Security Tips**
- **Q & A**

Introduction



- Computer Security protects your PC, and you
- It is never perfect but with care you can make your computer or on line account very hard to crack
- Wherever you use a computer, or access the internet, email, social media you will need to protect your computer with strong **passwords, firewalls** and **anti-virus programs.**
- If in doubt do not open an email or go to a website you are not sure about.
- Follow [Top Security Tips](#) slide & be as safe as you can



Downloading and applying updates to programs

- Security updates keeps your PC safe
- Microsoft automatic updates should be **ON**
 - You will need to be connected to internet to get updates
 - Updates from Microsoft should now occur automatically. Sometimes will require reboot of your PC. You can always go to START Menu and look for “Windows Update” and download manually-follow instructions-easy.
[Win7 example](#)
- Make sure Microsoft firewall is turned **ON**
- Other programs(e.g. Adobe, Firefox, Skype, Java, Flash etc)
 - All will have an option to update automatically
 - If not sure look under Help for “check for updates” & update manually
 - windows 7 just type update in start menu file box

Updates -More



- If a program suddenly opens a window or gives a message like “update available, update now” OR [User Access Control](#) Box
 - 1st check program name requesting is same as being used. Windows will often check this anyway.
 - Follow instructions, but if in doubt ask for help and cancel
 - If program tries to access critical parts of your computer your anti-virus/windows will likely popup telling you of this. If you have the choice select non-critical update or similar. If not decline and get advice.
- Using Anti-Virus security programs
 - Many anti-virus programs have an option to check all programs on your computer to determine what needs security updating and then point you at the correct place to get the update.
- Upgrade older security risky Programs by free download
 - From Outlook Express (XP) & Windows Mail (Vista) to [Windows Live Mail](#) or [Thunderbird](#).
 - From Internet Explorer 6 to [Internet Explorer 8](#), [Firefox](#) or [Chrome](#)

PC Firewalls



- PC's connected to the Internet without a **firewall** can be hijacked quickly. Remote PC's can then control your hijacked computer without you knowing.
 - Firewalls are designed to prevent unauthorized access/control to a PC or network.
 - All data sent to and from a system with a firewall is monitored and compared with a set of user-defined security criteria(definitions). Any data that does not meet those criteria is blocked.
 - There are two types of mutually complementary firewalls to consider.
 - **Host-based software firewalls** — software that protects the PC it is installed on.(e.g Windows Firewall, and/or anti-virus program firewall)
 - **Network-based hardware firewalls** — installed between your DSL or cable modem and your home network to protect all the computers on the network.
- Most High Speed Internet vendors(Bell, Rogers etc.) supply a combined Modem and Router(wireless or wired) box. The modem/Router box will contain a network hardware firewall.
- **Windows comes with a software firewall** which combined with the **hardware modem/Router firewall** is a good start
- In addition to Firewalls **every PC should have an anti-malware program(anti-virus)** for additional protection. These programs run in the background and attempt to catch virus's that may breach the firewall(s).

Securing DSL/Cable Modem/Routers

- **For the technically inclined.** However someone should do this for you following guidelines below.
- Securing a hardware **ethernet** firewall (router)
 - change the password
 - turn off remote management
 - turn off UPnP (Universal Plug and Play i.e. automatic port forwarding)
- Securing a **wireless** router
 - All of the above PLUS
 - implement WPA2 on the router and the clients (WEP isn't good enough any more) with a very strong password (20+ characters – gibberish)
 - change the default SSID
 - don't bother with MAC address filtering
 - don't turn off SSID broadcast (no extra security but performance loss)
 - use a VPN when forced to use WEP or an unsecured access point

Malware page 1 of 3



- **Trojan** - Software that appears to perform a desirable function for the user prior to run or install but instead facilitates unauthorized access of the user's computer system. *"It is a harmful piece of software that looks legitimate. Users are tricked into loading and executing it on their systems"* [Another example on Windows XP.](#)
- **Worm** - is a self-replicating malware program. It uses a computer network to send copies of itself to other PC's (computers on the network), and it may do so without any user intervention
- **Virus** - A computer virus is a computer program that can copy itself and infect a computer. The term "virus" is also commonly but erroneously used to refer to other types of malware, including but not limited to adware and spyware programs that do not have the reproductive ability.

Malware, short for *malicious software*, is software designed to secretly access a computer system without the owner's informed consent

Malware Page 2 of 3

- **Spyware** - is a type of malware that can be installed on computers, and which collects small pieces of information about users without their knowledge.
 - The presence of spyware is typically hidden from the user, and can be difficult to detect.
 - Designed to **steal personal info, identity theft and fraud**
- **Anti-spyware specific Programs** you can obtain include:
 - AdAware: [AdAware](#)
 - Spybot search and destroy: [spybot](#)
 - Spyware blaster: <http://www.javacoolsoftware.com/spywareblaster.html>
 - Microsoft Security Essentials : [MSE](#)
 - TrendMicro - [Trend](#) scan click on "Free spyware scan"

Malware Page 3 -3

- **Adware**, or **advertising-supported software**, is a software package which automatically plays, displays, or downloads adverts to a computer. .
- **Botnet** - is a collection of software agents, or robots, that run autonomously and automatically. The main drivers for botnets are for recognition and financial gain, often used for **denial of service attacks** on competitor websites and general spamming
- **Rootkit** - software that enables continued privileged access to a computer while actively hiding its presence from administrators by **subverting windows** operating system functionality .
- **Keystroke logging** (often called **keylogging**) is the action of tracking (or logging) the keys struck on a keyboard. Typically in a covert manner so that the person using the keyboard is unaware that their actions are being monitored. **Used to collect financial information**

Anti-virus & anti-spyware programs

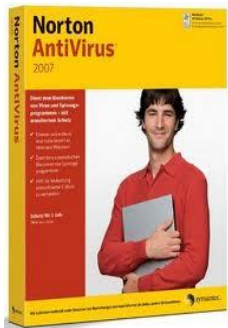


• Which one to choose, Free or Pay \$?

- Free: probably okay if no online banking
 - Free : [AVG Free](#) or [Microsoft Security Essentials](#)(MSE)
- Pay: then decide what features you need
 - Some do all, some just viruses or spyware
 - Most provide internet/email spam protection
- Best deal you can get
 - Often Banks will provide free if you use their online banking. Retail shops often have deals. Can often get 3 licences for price of one, so could share with a friend, or install on multiple computers.
 - Licence is usually for a year, sometimes longer

• Install more than one??

- Generally **should avoid** as conflicts occur
- Can run one real time, and others manually as required
- **ALWAYS UNINSTALL** old anti-virus before installing new one
- **IMPORTANT – Always do automatic definition updates**



Phishing - what it means and how to avoid



Phishing is the fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication. [Another Phishing](#) example via email.

- Communications purporting to be from popular social web sites, auction sites, online payment processors or IT administrators are commonly used to lure the unsuspecting public. **Phishing is typically carried out by e-mail or instant messaging**, and it often **directs users to enter details at a fake website** whose look and feel are almost identical to the legitimate one.
- Use an anti-virus program that protects from Phishing **PLUS** common sense.
- Always get in the habit of looking at the URL
- Browsers like IE or Firefox will have add-ons for anti-phishing
- If you receive an email or message **you are not sure about DO NOT click on it** but delete it and ask for advice.

Keyloggers - protecting your personal information



Keylogger spyware, also known as a keystroke logger, is a software application that captures and records each and every keystroke that is typed on your keyboard.

Protect Yourself by:

- Enable your [firewalls](#).
- Install anti-spyware and [anti-virus software](#).
- Obtain and use an automated form-filler, particularly if you often enter personal or financial information at any website. These form fillers encrypt and save this confidential information and automatically fill it in, so you won't have to type it in.
- Consider using an on screen keyboard. You would enter your information into this keyboard using your mouse rather than typing it in. Some Banks now employ this when you log in.
- Keep track of the programs that are running on your computer. Keyloggers tend to run in the background, out of sight. You can check the programs via the [Task Manager](#) by pressing (Ctrl + Alt + Delete).

Web Browser

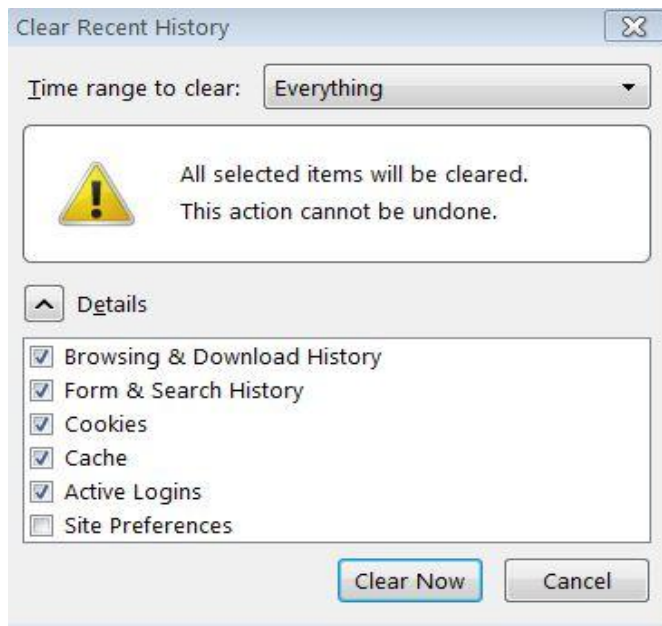
Cookies & safe web surfing



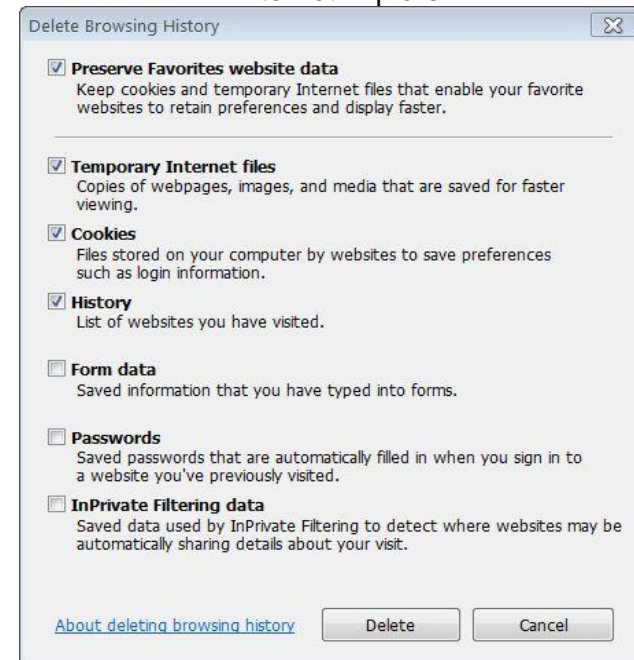
Cookies are mostly harmless

- convenience of remembering "state" eg. username/password
- tracking cookies so sites always load your preference e.g English rather than French layout
- You can get rid of them in Firefox:
 - Tools->Options->Privacy->Cookies->"for the originating web site only: set
- You get rid of them in Internet Explorer:
 - Tools->Internet Options...->Privacy->Settings:Advanced->Block
- Get in the habit BEFORE and AFTER using on-line banking when using Browsers to clear history:

Firefox

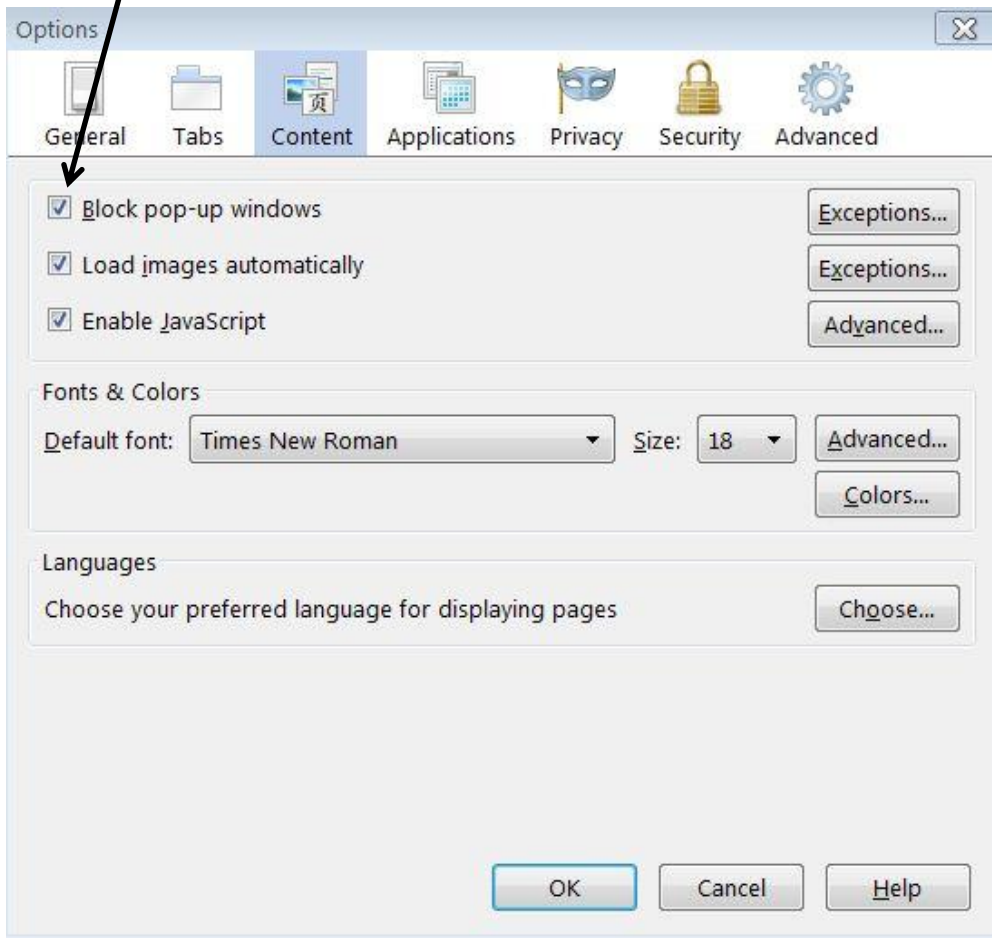


Internet Explorer

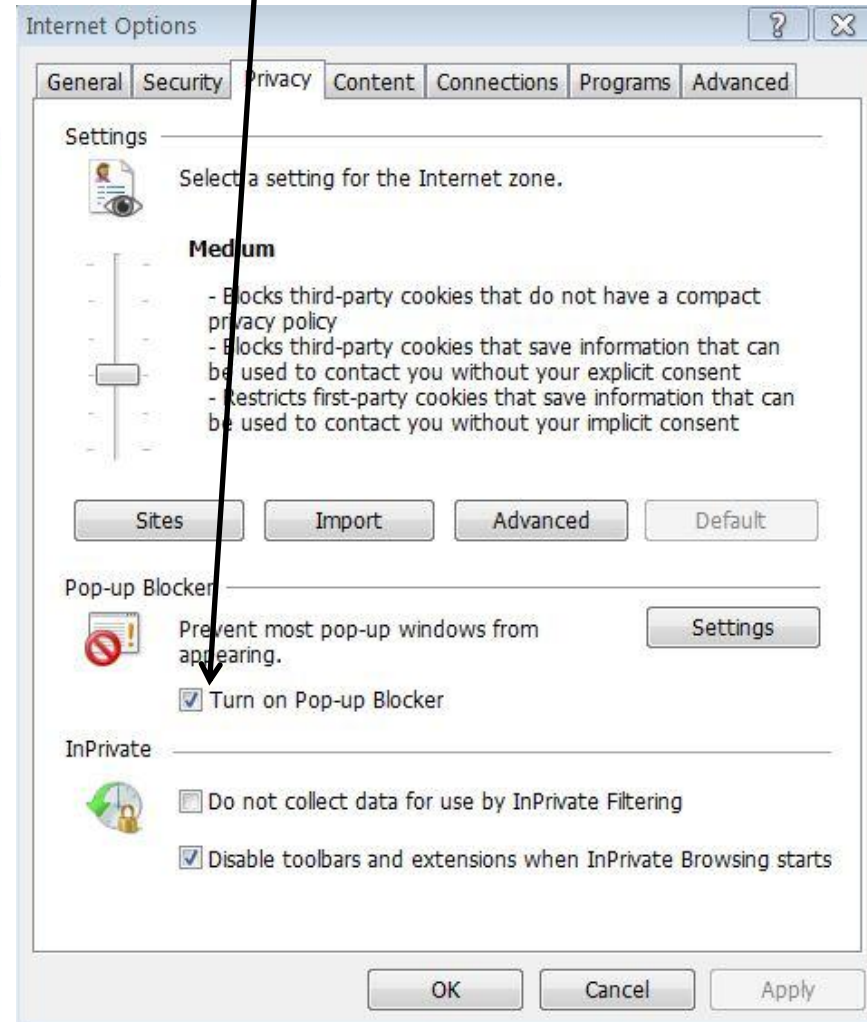


Web Browsing - Pop up Windows

Firefox(From Options)



Internet Explorer(From Options)



Handling Spam emails

Never respond to Spam

- Make sure Spam filters are turned on and check spam folder on a regular basis
- **Don't click on unsubscribe links.** - If you didn't originally sign up to receive the mail, or if you don't recognize the sender or company sending the email, then don't unsubscribe.
- **Don't publish your main email address** on any web site or discussion forum.
- **Use a separate email address** - to sign up for newsletters, online posting, and mailings. If the mailbox starts receiving an overabundance of spam, you can delete the mailbox or more aggressively filter it.
- **Purchase anti-spam software** - blocks 97-99% of spam to reduce the amount of spam you receive.
- **Use a good email program** like gmail that has built in anti-spamming
- **Do not reply to spam** and **Don't buy anything from spammers..**

Password selection and management

Your **passwords** are the keys you use to access personal information that you've stored on your computer and in your online accounts (email, banking, online retailers, Skype, facebook etc.)

How to make a strong password :

- **Make it lengthy.** 8 characters or more, mix upper lower case and use symbols like \$,%,&. More different characters the stronger the password . E.g. ``My\$Boat\$Is\$Blue! `` is stronger than ``joan1234``
- You can create a phrase made of many words (a "**pass phrase**") , separated by a symbol (_ , * , @ , # , ~ , etc.) or a number. A pass phrase is often easier to remember than a simple password. See Create a [strong password](#)
- Use words and phrases that are easy for you to remember, but **difficult for others to guess.**
- **Change Password** often– typically every 90 days

Password strategies to avoid

- **Avoid sequences or repeated characters.** "12345678," "222222," "abcdefg"
- **Avoid using only look-alike substitutions of numbers or symbols.** E.g. i for 1.
- **Avoid your login name.** Any part of your name, birthday, social security number, or similar information for your loved ones constitutes a bad password choice. - ie anything that may be in public domain.
- **Avoid simple dictionary words and different passwords for different systems**

Use a Password Manager to store multiple different passwords – see notes

– allows very strong passwords, unique password per site, E.g [onepass](#) or [Lastpass](#)

Keep your Passwords secret - no excuses

Please see [Password](#) slides at end for full details

Top Security Tips



- Security Scan your computer every week
 - Anti-virus Program and spybot (if not in anti-virus program) or Microsoft Security Essentials
 - Make sure to download latest virus definitions and latest anti-virus programs when available
- Always download and install security updates for Windows and browsers(IE ,Firefox etc.)
- Enable Microsoft Firewall and automatic updates
- Do Not open email attachment unless you know who its from. – see notes
 - Be wary of chain emails, as the originator may be infected
- Keep your user IDs and passwords confidential
- Create strong, effective passwords of 8 mixed characters or more
 - Change every 90 days, use different passwords for different accounts (e.g. email vs banking)
- Use a secure web browsing program such as Firefox, and enable strong security and privacy settings including the use of a pop-up blocker.
- Set up your email filters to delete or file spam messages.
- Back up your data to CDs or another storage medium on a regular basis.
 - If PC gets infected then may need to wipe complete PC Hard Disk &reinstall from CD's



Where to go to get more information

- <http://www.microsoft.com/protect/fraud/spam/email.aspx> - How to deal with suspicious email
- RCMP cyber-crime division - http://www.rcmp-grc.gc.ca/scams/index_e.htm - excellent tips
- RECOL: Report Economic Crime OnLine: <https://www.recol.ca> - examples of types of fraud
- check your credit history annually to make sure you have not been compromised. It's free!
 - Equifax: <https://www.equifax.ca/>
 - TransUnion: www.tuscores.ca
- an expert in the field http://www.schneier.com/blog/archives/2004/12/safe_personal_c.html

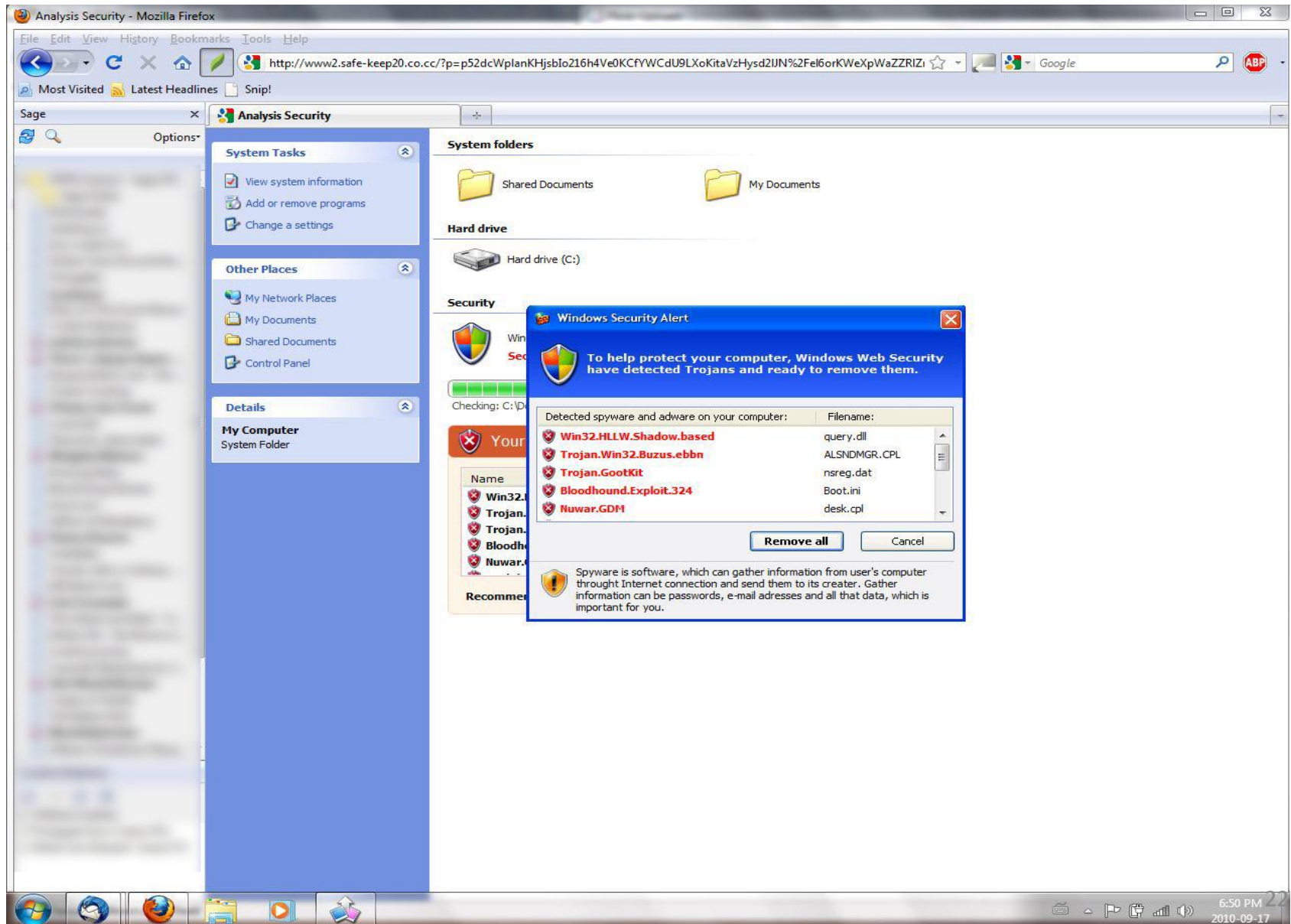
Q & A



- Please contact Steve Courtney at computer@kanataseniors.ca if you have any specific questions concerning computer security or computer problems . I may be able to help or direct you to someone who can.
- This presentation can be found at <http://www.kanataseniors.ca/pdf-files/Computers/security.pdf>

Supporting Slides Only

Trojan example



The screenshot shows a Windows XP desktop environment. A Mozilla Firefox browser window is open, displaying a webpage from www2.safe-keep20.co.cc. A Windows Security Alert dialog box is overlaid on the browser, indicating that Windows Web Security has detected Trojans and is ready to remove them. The alert lists the following detected spyware and adware:

Detected spyware and adware on your computer:	Filename:
Win32.HLLW.Shadow.based	query.dll
Trojan.Win32.Buzus.ebbn	ALSNDMGR.CPL
Trojan.GootKit	nsreg.dat
Bloodhound.Exploit.324	Boot.ini
Nuwar.GDM	desk.cpl

The dialog box also includes a "Remove all" button and a "Cancel" button. A warning icon and text at the bottom of the dialog state: "Spyware is software, which can gather information from user's computer through Internet connection and send them to its creator. Gather information can be passwords, e-mail addresses and all that data, which is important for you."

More Fake examples

[Examples of fake and real Windows XP Security Center](#)

The screenshot shows a Windows XP desktop environment. The main window is an Internet Explorer browser displaying a fake security scan page. The page title is "My computer Online Scan - Internet Explorer provided by Dell". The address bar shows a long, random URL. The page content includes:

- Hard Disc Drivers (2):** Local Disk (C:) with a progress bar and "Found 277 trojans"; Local Disk (D:) with a progress bar and "Found 43 trojans".
- Devices with Removable Storage (2):** Floppy Disk Drive (A:); CD Drive (E:).
- System scan progress:** A green progress bar and the text "Scan complete. 320 fileinfos was found!".
- Your Computer is Infected!** A red banner with a shield icon.
- Table of detected threats:**

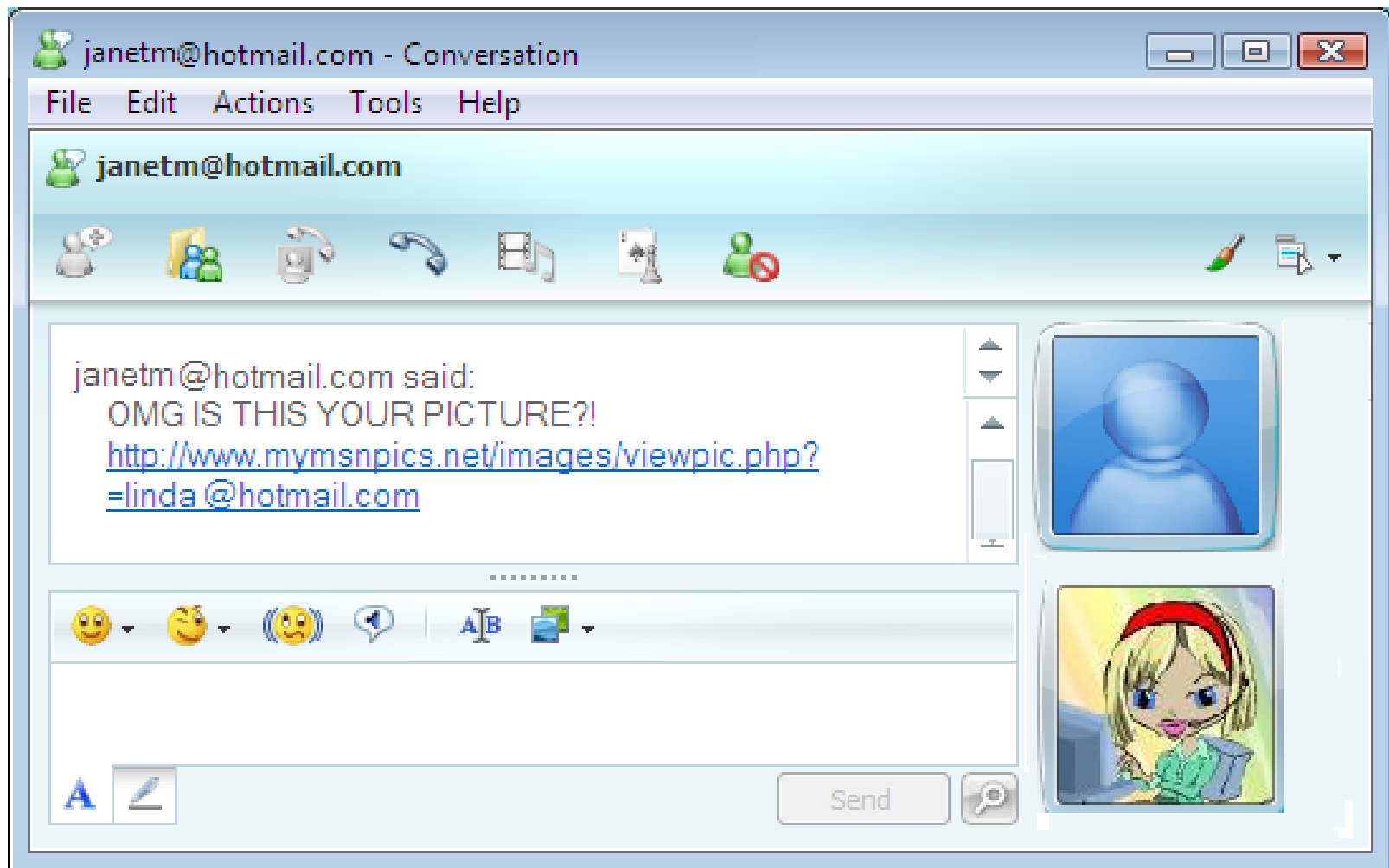
Name	Risk level	Details
Email-Worm.Win32.Net	Critical	
Email-Worm.Win32.Myd	Critical	
Trj-Dwnldr.Win	Critical	3/17/2009 2 Waiting removal
Email-Worm.Win32.Eyeveg.b	Critical	2/13/2010 5 Waiting removal

Below the table is a "Security" section with a red bar and the text "Virus protection (Important) Windows did not find antivirus software on this computer. Turn off messages about virus protection." and a "Find a program online" button.

A "Windows Security Alert" dialog box is open in the foreground. It features a yellow warning icon and the text: "To help protect your computer, Windows Defender has detected spyware and ready to remove them." Below the text are "Remove all" and "Cancel" buttons. A larger text box explains: "Spyware is software which is loaded onto your computer without your knowledge, or possibly without the full functionality being made clear to you. It can, among other things, slow your internet connection down and make frustrating changes to your browser."

The taskbar at the bottom shows the Start button, the name "Don", and several open applications: "My computer Onlin...", "Write: (no subject)", and "Inbox - Mozilla Thu...". The system tray on the right shows "Internet | Protected Mode: On", a volume icon, and the time "4:07 PM".

Worm Example



[back](#)

Don't know who linda@hotmail.com is so DONOT click on the link

Virus example



[back](#)

Adware example

The image displays a dense collection of overlapping web advertisements and browser windows. Key elements include:

- Top Left:** A purple and blue advertisement for BT (British Telecom) with the text "Free connection Free modem Click here to find out more".
- Top Center:** A red and white advertisement for Xerox with the headline "Enter to WIN! XEROX WIN an \$11,000 USD Business Upgrade Package or a Xerox Phaser® 8400 Color Printer". It also features the text "World's fastest color printer for under \$1,000 USD. Phaser 8400 Color Printer \$999".
- Top Right:** A blue advertisement for PC World with the text "TRY 2 RISK-FREE ISSUES! GET 15 FREE".
- Middle Left:** A large blue and white advertisement for AOL broadband with the headline "Before you go, did you know.... You can add AOL® for Broadband to any high-speed cable or DSL connection!". It lists benefits like "Works with and enhances any basic high-speed connection" and "Built-in protection for you and your family". It includes a "GET A FREE TRIAL! Up to 45 days FREE" offer and a "Click here for details" button.
- Middle Center:** A white advertisement for Ameriquest Mortgage Company with the headline "Home-Owners Click Here" and "AMERIQUEST MORTGAGE COMPANY®".
- Middle Right:** A yellow advertisement for Netscape with the headline "What's New" and a list of news items: "Science Proves It: Drinking Causes...", "Teen Girls Beware: Popular Boys Do THIS", "Look What Was Found in Stone Age Cave", "Strange Space Object Mystery Deepens", "Did You See What Bush Dared to Wear?", and "If You Get This E-Mail Scam, Delete It".
- Bottom Left:** A white advertisement for ReliaQuote with the headline "ReliaQuote A better way to buy life insurance" and "Save up to 70% on life insurance".
- Bottom Center:** A white advertisement for TravelZoo with the headline "TRAVELZOO™" and "This Week's Top on the Internet Released APRIL 14".
- Bottom Right:** A green advertisement for HomeLoanCenter.com with the headline "Rates are at Historic Levels" and "Get cash your home". It features an image of a house made of money.

[back](#)

Spyware example – Detected by Spybot

The screenshot shows the Spybot - Search & Destroy application window. The title bar reads "Spybot - Search & Destroy". The menu bar includes "File", "Mode", "Language", and "Help". The main window has a sidebar on the left with icons for "Search & Destroy", "Recovery", "Immunize", "Update", and "Donations". The main area is titled "Search & Destroy" with the subtitle "Scan for problems and remove them." Below this are buttons for "Check for problems", "Fix selected problems", "Print", and "Help". A message with a binoculars icon states: "This is the main scan page of Spybot-S&D. Here you scan your system ('Check for problems' button) and fix any problems found ('Fix selected problems' button). Hint: if you haven't done so yet, we recommend you read the tutorial (see Help menu) to learn how to deal with the scan results." Below the message is a "Hide this information" link. A table lists detected problems:

Problem	Kind
<input checked="" type="checkbox"/> bluestreak	1 entries
<input checked="" type="checkbox"/> DoubleClick	1 entries
<input checked="" type="checkbox"/> FastClick	1 entries
<input checked="" type="checkbox"/> HitBox	2 entries
<input checked="" type="checkbox"/> KillSec	1 entries
<input checked="" type="checkbox"/> MediaPlex	1 entries
<input checked="" type="checkbox"/> Statcounter	1 entries
<input checked="" type="checkbox"/> Zedo	1 entries

The "DoubleClick" entry is selected, and a detailed view is shown on the right:

- Company:** DoubleClick
- Product:** Cookie
- Threat:** Tracking cookie or cookie of tracking site
- Company URL:** <http://www.doubleclick.com>
- Company privacy URL:** http://www.doubleclick.com/us/corporate/privacy/privacy/default.asp?asp_object_1=&

At the bottom left, it says "12 problems found (17:23)". A watermark "www.stapiles.com" is visible in the bottom right of the interface.

[back](#)

Phishing Examples



bmo.com | site map | contact us | locate us | francais | 中文



bmo.com | site map | contact us | locate us | francais | 中文

BMO Bank of Montreal

Personal Finances Sign In

[Home](#) [Accounts & Plans](#) [Mortgages](#) [Loans & Credit Cards](#) [Investments](#) [Insurance](#) [Online Banking](#) [Rates](#)

[Sign In](#) [Take a Tour](#) [FAQs](#) [Register Now](#) [Security Tips](#) [Technical Requirements](#)

Sign In to Online Banking

Ouverture de session

Bank Card: 500766 Password:

[Remember my Bank Card](#)

[Forgotten Password?](#)

Tools & Info

- [When not to save your Bank Card](#)
- [What's new in Online Banking](#)
- [Register Now](#)
- [Online Banking Tour](#)

[back](#)

Phishing example 2



Dear Customer

We value your relationship with Bank of Montreal To serve you better,we are installing the Best Banking software and would require you Update Your Online Banking Records.

This is being done to secure your accounts and to protect your personal informations from being compromised.We at Bank of Montreal are committed in making sure that your online transactions are secure.

Click on the link below to Update your Account Records

[ht tps://www.Online Banking Log-In/rdcLogin/?RXZlbnQzIERlYzA3](https://www.Online Banking Log-In/rdcLogin/?RXZlbnQzIERlYzA3)

Once your information has been updated and confirmed your online service would continue as usual and would not be interrupted

Sincerely,
Bank of Montreal
Online Customer Service

[back](#)

Passwords 1 of 2

How to make a strong password

- **Make it lengthy.** Each character that you add to your password increases the protection that it provides many times over.
- Your passwords should be 8 or more characters in length; 14 characters or longer is ideal.
- You can create a phrase made of many words (a "pass phrase"), separated by a symbol (_ , * , @ , # , ~ , etc.) or a number. A pass phrase is often easier to remember than a simple password, as well as longer and harder to guess.

- **Combine letters, numbers, and symbols.** The greater variety of characters that you have in your password, the harder it is to guess.
 - **The fewer types of characters in your password, the longer it must be.** 15-character password composed only of random letters and numbers is about 33,000 times stronger than an 8-character password composed of characters from the entire keyboard. If you cannot create a password that contains symbols, you need to make it considerably longer to get the same degree of protection. An ideal password combines both length and different types of symbols.
 - **Use the entire keyboard,** not just the most common characters. Symbols typed by holding down the "Shift" key and typing a number are very common in passwords. Your password will be much stronger if you choose from all the symbols on the keyboard, including punctuation marks not on the upper row of the keyboard, and any symbols unique to your language.

Other important specifics include:

- **Use words and phrases that are easy for you to remember, but difficult for others to guess.**

The easiest way to remember your passwords and pass phrases is to write them down. Contrary to popular belief, there is nothing wrong with writing passwords down, but they need to be adequately protected in order to remain secure and effective. In general, passwords written on a piece of paper kept away from system access devices are more difficult to compromise across the Internet than a password manager, Web site, or other software-based storage tool.

How to access and change your passwords

The Help files for your computer operating system will usually provide information about how to create, modify, and access password-protected user accounts, as well as how to require password protection upon startup of your computer. You can also try to find this information online at the software manufacturer's Web site. For example, if you use Microsoft Windows XP, online help can show you how to manage passwords, change passwords, and more.

Keep your passwords secret

Treat your passwords and pass phrases with as much care as the information that they protect.

if you have to write them down, consider a password "safe" with a master password that's not written down e.g. keyring for the palm or KeePass for windows See (<http://keepass.sourceforge.net/>)

- use <https://www.grc.com/password> to generate crypto secure passwords
- use lastpass <http://lastpass.com/>

[back](#)

Passwords 2 of 2

Create a strong, memorable password in 3 or 4 steps

Use these steps to develop a strong password:

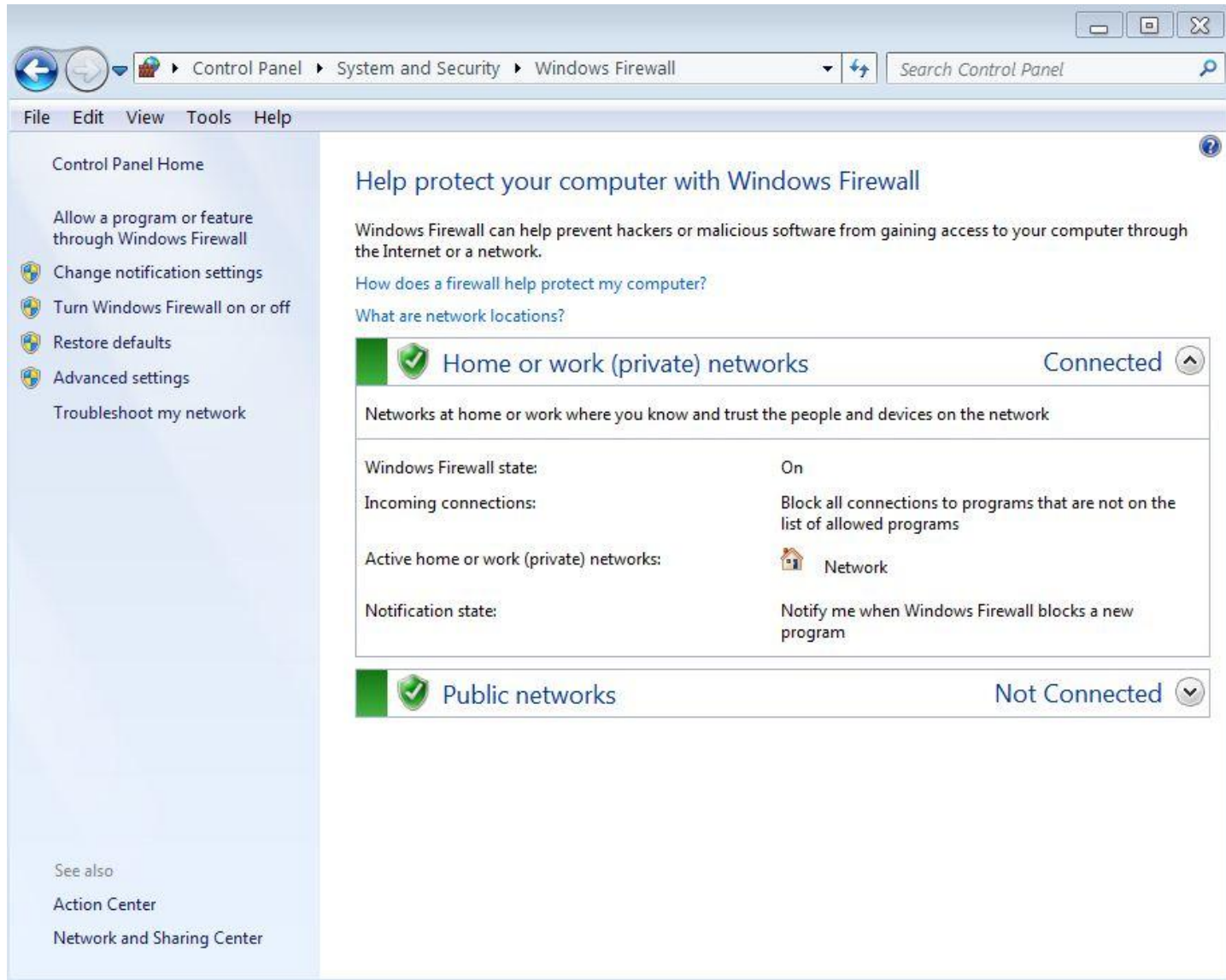
- **Think of a sentence that you can remember.** Use a memorable sentence, such as "My grandson Aiden is three years old this year"
- **Convert the phrase to a password.** Take the **first** letter of each word of the sentence that you've created to create a new, nonsensical word. Using the example above, you'd get: "mgaioty".
- **Add complexity** by mixing uppercase and lowercase letters and numbers. This might yield a password like if you always say change the 1st letter to upper case "Mgai3oty". This is now a strong password.
- **Finally, you could substitute some special characters to make the password even stronger.** You can use symbols that look like letters, combine words (remove spaces) and employ other ways to make the password more complex. E.g substitute "\$" for "y" and you get "mgait\$ot\$"

Password strategies to avoid

Some common methods used to create passwords are easy to guess by criminals. To avoid weak, easy-to-guess passwords:

- **Avoid sequences or repeated characters.** "12345678," "222222," "abcdefg," or adjacent letters on your keyboard do not help make secure passwords.
- **Avoid using only look-alike substitutions of numbers or symbols.** Criminals and other malicious users who know enough to try and crack your password will not be fooled by common look-alike replacements, such as to replace an 'i' with a '1' or an 'a' with '@' as in "M1cr0\$0ft" or "P@ssw0rd". But these substitutions can be effective when combined with other measures, such as length, misspellings, or variations in case, to improve the strength of your password.
- **Avoid your login name.** Any part of your name, birthday, social security number, or similar information for your loved ones constitutes a bad password choice. This is one of the first things criminals will try.
- **Avoid dictionary words in any language.** Criminals use sophisticated tools that can rapidly guess passwords that are based on words in multiple dictionaries, including words spelled backwards, common misspellings, and substitutions. This includes all sorts of profanity and any word you would not say in front of your children.
- **Use different passwords for different systems.** If any one of the computers or online systems using this password is compromised, all of your other information protected by that password should be considered compromised as well. It is critical to use different passwords for different systems.

Win 7 Firewall



The screenshot shows the Windows Firewall control panel window. The title bar indicates the path: Control Panel > System and Security > Windows Firewall. The window has a menu bar with File, Edit, View, Tools, and Help. On the left is a navigation pane with links: Control Panel Home, Allow a program or feature through Windows Firewall, Change notification settings, Turn Windows Firewall on or off, Restore defaults, Advanced settings, and Troubleshoot my network. The main content area is titled 'Help protect your computer with Windows Firewall' and contains introductory text, links for help, and a summary of network locations. The 'Home or work (private) networks' section is expanded, showing the firewall is 'On' and 'Incoming connections' are blocked. It also lists one active network and the notification state. The 'Public networks' section is collapsed.

Control Panel > System and Security > Windows Firewall

File Edit View Tools Help

Control Panel Home

Allow a program or feature through Windows Firewall

Change notification settings

Turn Windows Firewall on or off

Restore defaults

Advanced settings

Troubleshoot my network

Help protect your computer with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or a network.

[How does a firewall help protect my computer?](#)

[What are network locations?](#)

Home or work (private) networks Connected

Networks at home or work where you know and trust the people and devices on the network

Windows Firewall state:	On
Incoming connections:	Block all connections to programs that are not on the list of allowed programs
Active home or work (private) networks:	Network
Notification state:	Notify me when Windows Firewall blocks a new program

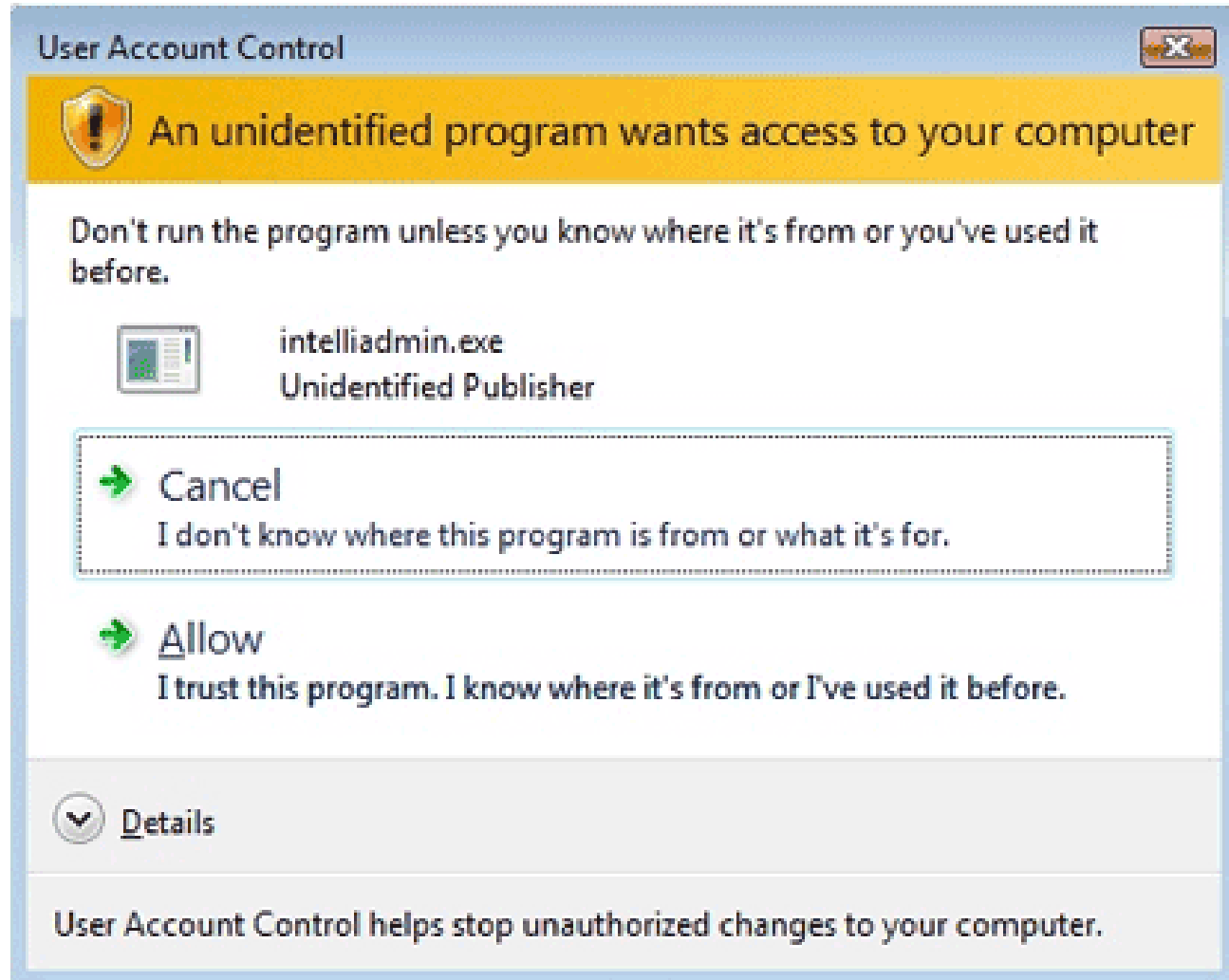
Public networks Not Connected

See also

Action Center

Network and Sharing Center

UAC



Win7 Updates ON

