

Computer Security

In this section you will learn about different types of security threats and how to reduce your risk. Also privacy issues that are relevant to security will be discussed.

Test

- You get a file attachment in a message, from which of the following people would should you accept it and why?



A total stranger



Someone you've only met on the Internet

Colourbox.com



Your best friend

Colourbox.com



This guy!!!

Examples

From: James Tam
(tamj@cpsc.ucalgary.ca)
To: All students
Subject: Surprise gift

Hi this is your course instructor. Everyone is a winner in my classes...you all get A+!

[Click here to get your grade](#)

Bottom Line

- Don't automatically trust any suspicious emails with links or attachments regardless of who the source may appear to be

Hacker

- A generic term for a person that writes malicious software (e.g., a virus that damages your computer) or tries to break into a computer system.



From: www.colourbox.com

One of many examples today: "Hacker attack leaves women angry, worried"

A security breach that exposed such personal information as the addresses and birth dates of more than 160,000 women enrolled in a mammography registry is raising questions about protecting people's privacy while at the same time making information available for much-needed research, an expert on bioethics said....

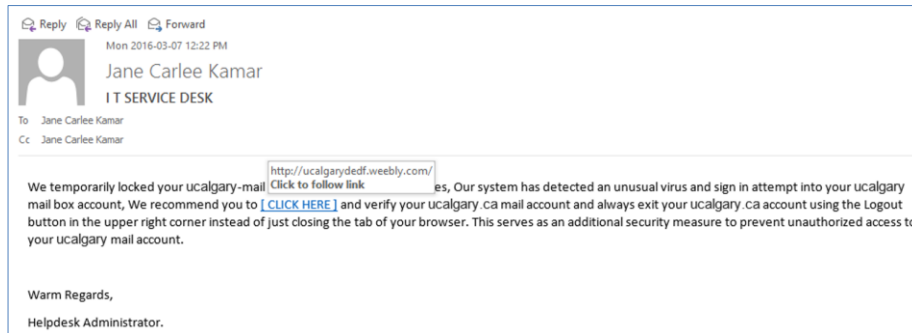
...from the Winston Salem Journal

"Hacked" Computer System

- Refers to a computer system in which the security system has been compromised.
 - "...to gain access to a computer illegally" (www.m-w.com)
 - "To use one's skill in computer programming to gain illegal or unauthorized access to a file or network" (<http://www.thefreedictionary.com>)
 - Allow access to the data on the computer(s)
- It can be done in many ways:
 - Sometimes it's as simple as getting an administrator password
- Sometimes this term is used in popular culture (even by news media outlets) for less serious security issues.

Phishing

- An attempt to get another person to reveal personal or confidential information (such as passwords) through trickery.



How Many “Fall For It”?

- Too many
 - Gartner estimates that 57 million U.S. Internet users have received fraudulent e-mail linked to phishing scams, and that 3% of them, or 1.7 million people, may have been tricked into divulging personal information.¹
 - (In contrast the “click through” rate of general spam junk email is just one half of a percent.²
 - Other sources provide a far gloomier picture (statistics sent to me via an university email from UC-IT)
 - “On average, 12-30 per cent of users open malicious emails and then click on a link in the email. Companies that provide training programs notice improvements of between 26 and 99 per cent in their phishing email click rates.”³
 - It’s serious enough at this university such that ALL faculty and staff will be tested!

¹<https://www.computerworld.com/securitytopics/security/cybercrime/story/0,10801,92948,00.html> (Last accessed Nov 20, 2017)

²<https://www.computerworld.com/article/2564850/cybercrime-hacking/surge-in-phishing-attacks-prompts-calls-for-change.html> (Last accessed Nov 20, 2017)

³ (Ponemon 2016 report, <https://securityintelligence.com/cost-of-a-data-breach-2016/>)

Basic/Simple Phishing Example

- You have a problem with unauthorized access and you need to login to *confirm access*.
- Apply a common sense filter to this:
 - One good negates several bad?

Slightly Better Phishing Attack

- “Spear phishing¹”: make the message more convincing by:
 1. Targeting the members of a particular organization (e.g. U of C staff and faculty, customers of an online business etc.)
 2. The email appears to originate from this organization.
 - (In some cases the actual mail server of the organization may have been previously compromised and used to send these emails).
- Using these above two techniques the email then provides urgent and apparently legitimately sounding reasons why personal data must be provided by going to a website (with a conveniently provided link in the email) where there is a request or requests for private information: passwords, pins, login names etc.

¹ FBI (US Federal Bureau of Investigations):
https://archives.fbi.gov/archives/news/stories/2009/april/spearphishing_040109

How You Can Get Stung With A Phishing Email?

- Obvious level: you gave given away private information
- Less obvious: you go to the website just to “check it out” but you don’t give any private information.
 - No problem?
 - Think again!
 - Your computer/phone can be infected by simply visiting a website.
 - Going to a website downloads the ‘content’ (text, images, videos etc.) but may also download programs (in the form of ‘scripts’).
 - Skeptical? Try going to this web address:
 - <https://pages.cpsc.ucalgary.ca/~tami/2017/203F/autorun.html>

Scripts? Who Needs Them! ...Likely You Do

The image is a collage of browser screenshots illustrating JavaScript requirements and security warnings. The top left shows a Facebook page with a "JavaScript Required" error message: "We're sorry, but Facebook doesn't work properly without JavaScript enabled." The top right shows a YouTube page with a yellow "A-OK!" box. The bottom left shows a Google Maps warning: "When you have eliminated the JavaScript, whatever remains must be an empty shell. Enable JavaScript to see Google Maps." The bottom right shows a browser window for "my.ucalgary.ca" with a "Detecting if CAS authentication is required..." message.

Denial Of Service Attack

- An attempt to make a service unavailable
 - Repeatedly sending requests for information to the computer system
 - “Crashing” the computer system that is under attack
- The ‘attackers’ (owners of the computer(s) from which the attack has been launched) may be unaware of their involvement
 - “Mydoom/MyDoom” infected computers
- Symptoms
 - Computer running more slowly
 - Some processes taking up resources (processor time, memory – Task manager)
 - Increase in network usage (ISP)

How Do The Following Affect Your Security?

- My financial institution/workplace/university computer system has been:
 - Hacked?
 - Suffered from a Denial of service attack?
 - <http://montrealgazette.com/news/local-news/youve-been-hacked>

You've been hacked!

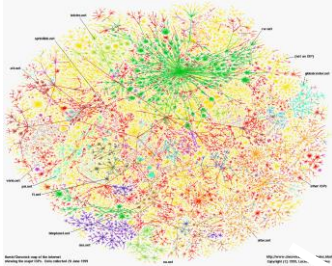
There are many examples, both big and small, of data security breaches in Canada.

(Exert)

“Hacktivists temporarily overwhelmed a number of federal websites with denial-of-service attacks to oppose the government’s anti-terrorism bill, C-51.”

- Users of my financial institution/workplace/university computer system have fallen for a phishing scam?

How To Guarantee Security Against Threats Such As Viruses



Disconnect your computer from the Internet

Leave your computer and devices off all the time

Put your computer in a vault



From: www.colourbox.com

How To Guarantee Security Against Threats Such As Viruses (2)

- “Simple”: just buy a brand new computer!
- Think again!



A major security flaw has been discovered in Lenovo's consumer PCs.

New Lenovo PCs shipped between September and December were pre-installed with adware known as Superfish, which uses a man-in-the-middle certificate to

From PC mag (2015): <http://www.pcmag.com/article2/0,2817,2477006,00.asp>

How To Guarantee Security Against Threats Such As Viruses (3)

- “Simple”:
 - “Simple solution #1”: Just ‘nuke’ my computer (wipe all the drives and reinstall everything)
 - “Simple solution #2”: Use a computer with an operating system other than MS-Windows like MAC-OS or Linux.

Computer hardware (i.e. not MS-Windows specific) can be infected with malicious software)

- This ‘infection’ cannot be removed by formatting the hard drive
- From
- <http://www.forbes.com/sites/thomasbrewster/2015/03/18/hacking-tails-with-rootkits/>

For more information on ‘infecting’ computer hardware with malicious software (CanWest security conference 2015)
<https://cansecwest.com/agenda.html>

How To Guarantee Security Against Threats Such As Viruses (4)

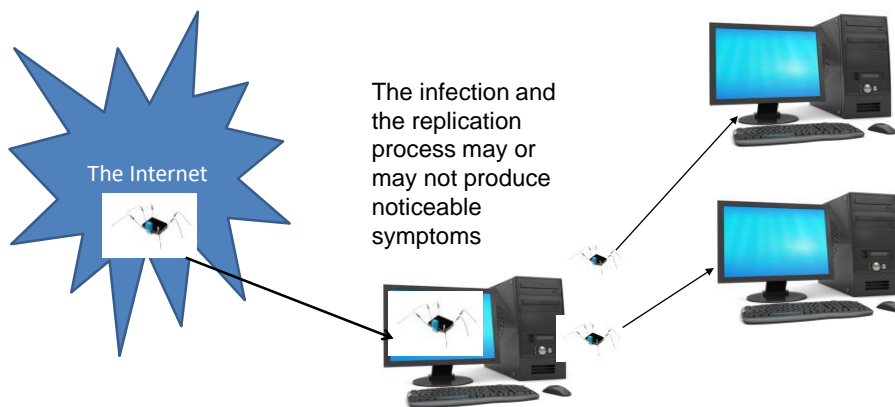
- Lesson:
 - You are never guaranteed to have 100% protection.
 - Taking precautions (e.g., getting anti-virus software) provide a *reduced* chance of an infection or other security-related problem.

Malware (“Malicious Software”)

- A program designed to infiltrate or damage a computer.
- Most references to computer viruses are actually references to malware.
 - The distinction is important because programs written to protect you from a virus may not offer you full protection against other forms of malware (you need a specialized program)
- Categories of Malware:
 - Computer viruses
 - Worms
 - Macro Viruses
 - Trojans / Trojan Horses
 - Spyware
 - Note: there is much overlap between these categories e.g., a Trojan may also include spyware.

Computer Virus

- Similar to a biological virus

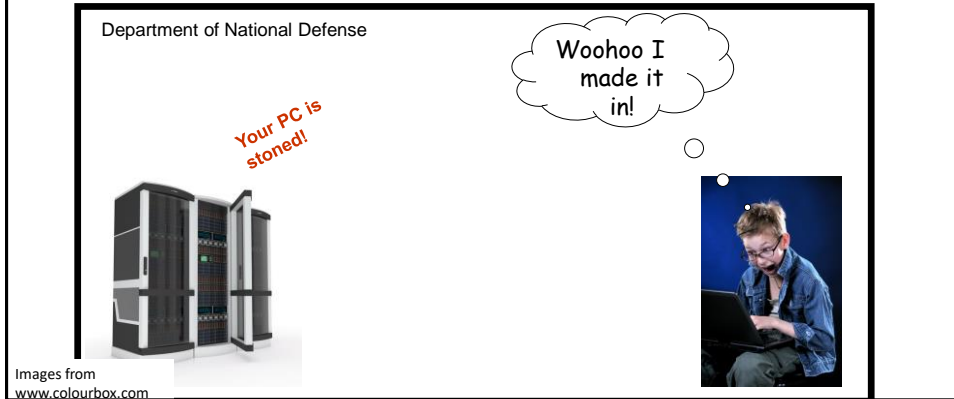


Images from: www.colourbox.com

Computer Virus: Objective

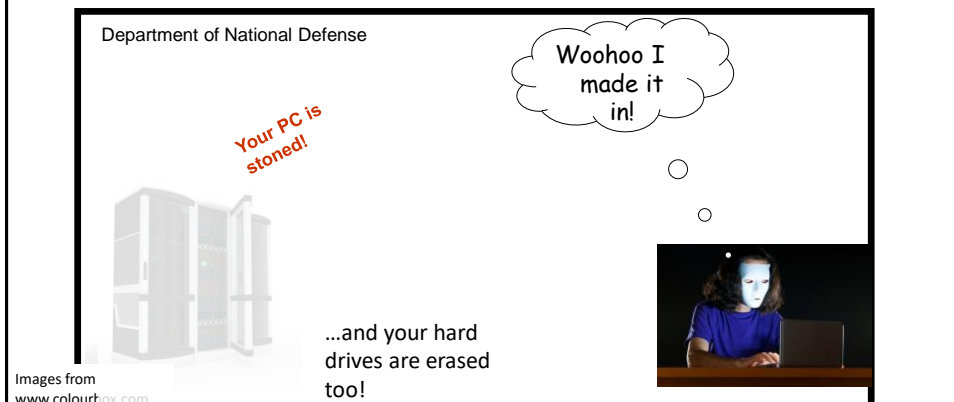
- For early virus writers the goal was simply infiltration of a computer or network.

At most the virus would result in some minor mischief



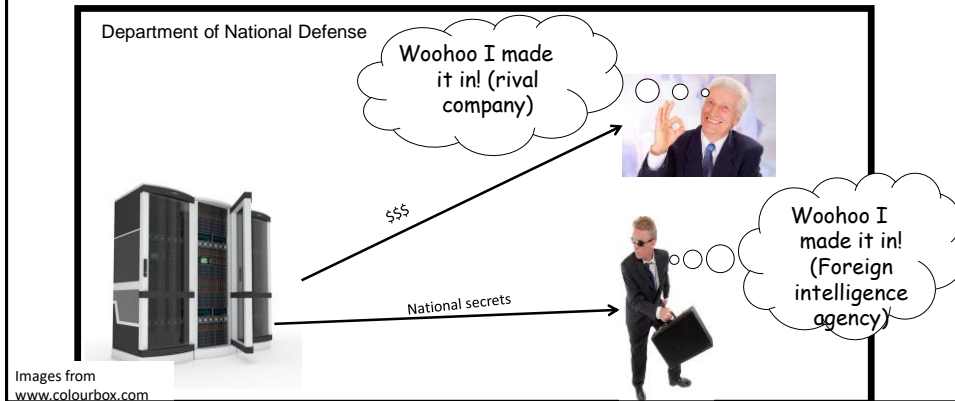
Computer Virus: Objective (2)

- Some viruses were designed to be malicious or were 'mutated' into a malicious version.



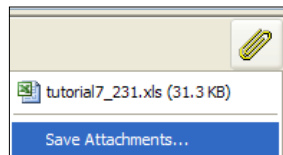
Computer Virus: Objective (4)

- Now a virus infection may be related to business or national espionage.
 - This means that ‘serious’ resources can be put into ‘hacking’.

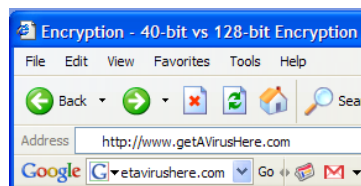


Computer Virus: Spread

- Require human-intervention to spread:
 - Opening email attachments



- Web-based: just going to a website can result in a infection “drive-by download”



I Can't Get Infected Just Going To A Website!

– Don't believe you can be infected, remember this one:

- <https://pages.cpsc.ucalgary.ca/~tami/2017/203F/autorun.html>

“Top 10 Celebs [JT: Searching For Info. About Them] Most Likely To Give You A Computer Virus”¹

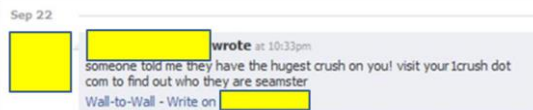
2013	2012	2011
1) Lily Collins	1) Emma Watson	1) Heidi Klum
2) Avril Lavigne	2) Jessica Biel	2) Cameron Diaz
3) Sandra Bullock	3) Eva Mendes	3) Piers Morgan
4) Kathy Griffin	4) Selena Gomez	4) Jessica Biel
5) Zoe Saldana	5) Halle Berry	5) Katherine Heigl
6) Katy Perry	6) Megan Fox (up from #15!)	6) Mila Kunis
7) Britney Spears	7) Shakira	7) Anna Paquin
8) Jon Hamm	8) Cameron Diaz	8) Adriana Lima
9) Adriana Lima	9) Salma Hayek	9) Scarlett Johansson
10) Emma Roberts	10) Sofia Vergara	10) Tie! Emma Stone, Brad Pitt and Rachel McAdams

¹ Source: <http://www.mcafee.com/us/microsites/most-dangerous-celebrities/index.html>

Computer Virus: Avoiding?

- “Solution”: Just don’t go to *bad* websites
 - “Trusted websites may inadvertently be used as part of a virus attack.
- Examples:
 - Facebook Virus Infecting 'Friends' List: Prompts Users to Download Video
 - <http://www.canada.com/globaltv/ontario/story.html?id=48291ac4-f3c5-465c-b172-80299e4ca5dc>
 - Provocative messages from your contacts that tempts viewers to follow a link:

Legitimate message from a friend or a virus?

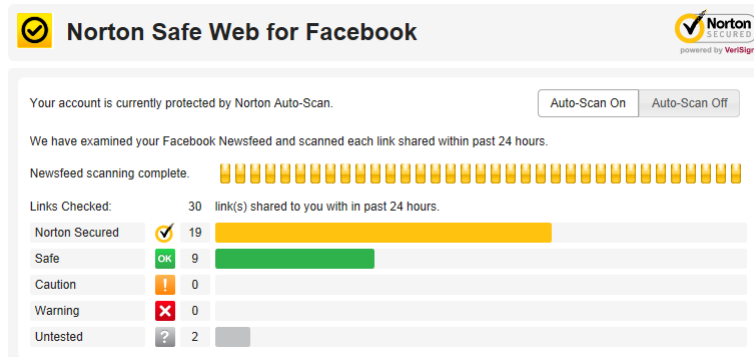


Computer Virus: Avoiding?

- Also it’s not just personal accounts that can be hacked but also the entire website itself or the company’s computers/database.
 - <http://www.ibtimes.com/hacks-cost-sony-pictures-entertainment-15-million-investigation-cleanup-costs-1850048>
 - <http://money.cnn.com/2014/01/10/technology/security/target-hack-tips/index.html>
- The means you can get infected by just visiting one of your favorite websites (without clicking on potentially malicious links)

Useful Side Note: Evaluating Security Of Facebook Links

- A Facebook security app



Worms

- Unlike a virus a Worm can spread without human intervention.
 - Many worms have automatically infected computers e.g., 'Slammer' (2003)

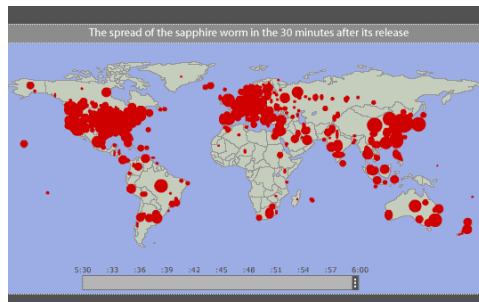


Image and facts from www.pbs.org (Accessed in 2015)

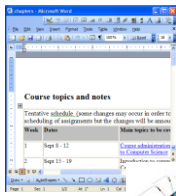
- At it's peak Slammer doubled in size every 8.5 seconds
 - Within 10 minutes it infected 90% of the worlds vulnerable host computers
- For detailed information (Symantec anti-virus)
 - http://www.symantec.com/security_response/writeup.jsp?docid=2003-012502-3306-99

Worm: Consequences Of An Infection

- Worms are designed to automatically spread themselves (ties up computer resources trying to infect other computers).
- They may have other negative effects similar to a virus.
 - “My computer is so slow”
 - My computer is acting ‘funny’

Macro Viruses

- Macros can be added to many types of documents.
 - They provide useful functions e.g., allow for some tedious tasks to be automated.
- A macro virus is a malicious program that’s imbedded as a macro in a file.
- Macro viruses replicate through the application that’s associated with the file (e.g., an MS-Word document).



Original document: infected



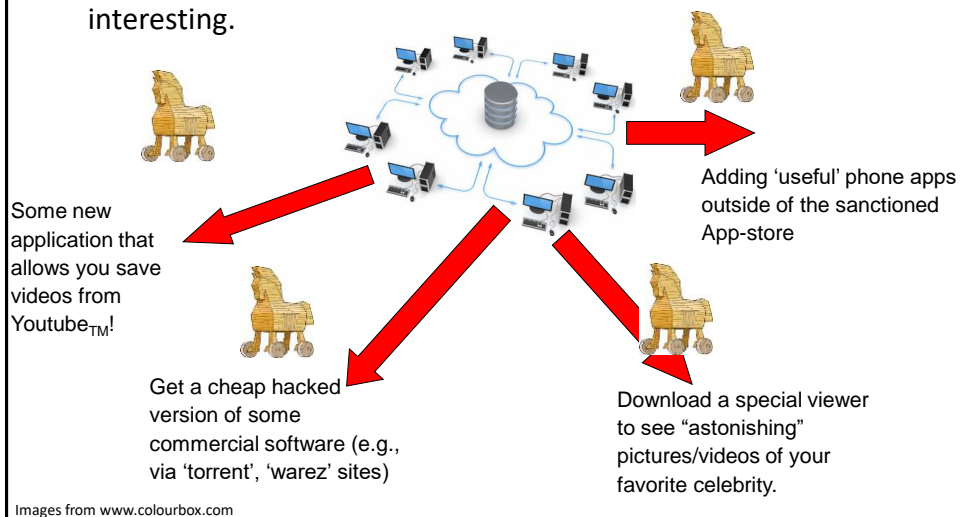
Documents made with that application contain the infection

Consequences Of Getting A Macro Virus Infection

- Not only the original infected document spawns infections but ANY document created with that application is infected if the 'template' document e.g., 'Normal.dot' has been compromised
 - (An example from VBA programming)
 - **Word macro that adds the Normal template to the collection of currently opened documents (where it may be edited by the macro).**
 - `Set wordDocument = Documents.Add("Normal.dot")`

Trojans / Trojan Horse

- They are imbedded in a program or file that looks useful or interesting.



Consequences Of A Trojan Infection

- A Trojan tricks users into infecting their computer by “letting in” the malicious program
 - E.g., you install what you think is a useful program only to have a malicious program bundled in
- The backdoor program can have negative effects similar to a virus infection.

Protection Against These Forms Of Malware

- Malware discussed so far
 - Viruses
 - Worms
 - Macro Viruses
 - Trojans / Trojan Horses

Protection Against These Forms Of Malware

- Use an anti-virus program:
 - It's included in Windows 'for free':
 - Windows (Windows security essentials is available for free download while Windows defender is built into Windows 8+):
<http://windows.microsoft.com/en-CA/windows/security-essentials-download>
 - If your operating system doesn't include security software
 - Something is better than nothing (some are free!)
 - Many Internet providers give something out for free if you're a subscriber
 - But try to get a program from an established company (better than a free version or a version produced by a smaller or less experienced company).
 - McAfee: <http://www.mcafee.com>
 - Norton: <http://www.norton.com>
 - Kaspersky: www.kaspersky.com
 - But make sure that you *update your program and the virus definitions* on a regular basis.

Spyware



From www.colourbox.com

- Secretly gathers information about your computer and computer usage and transmits this information back to the author.
- In some cases the process may be fairly legitimate in other cases it may be more nefarious.
- Spyware may also take the form of a program that is installed with another (potentially useful) program making it similar to a Trojan.

From the software usage agreement from some company 'X':

(From Internet Privacy for Dummies "The first spyware?")

"You hereby grant company X [*JT: actual name removed*] the right to access and use the used computing power and storage space on your computer/s and/or Internet access or bandwidth for the aggregation of content and use in distributed computing."

Spyware (2)

- Some forms of spyware are relatively benign and record generic information about your computer.
- However some forms of spyware record and transmit *highly* confidential information.
 - Some do this by recording and sending all the text that you enter with the infected computer.
 - Others may be more selective (e.g., it recognizes when you're about enter information into a password field and only send passwords and other login information).
 - A few may even transmit as a live video your computer desktop and send the video to the creator of the spyware.



From www.colourbox.com

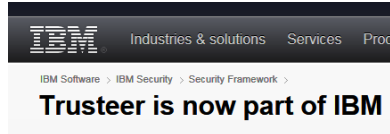
What Does Spyware Information Look Like?

- A program that records to a file what you are currently doing on your computer.
- (This is not meant as 'spyware' but instead is used to help troubleshoot technical problems.
 - "What did the user do?"
 - (Windows 7: Problem Steps Recorder)
 - (Windows 10: Steps Recorder or PSR)

Banking Anti-Spyware Software

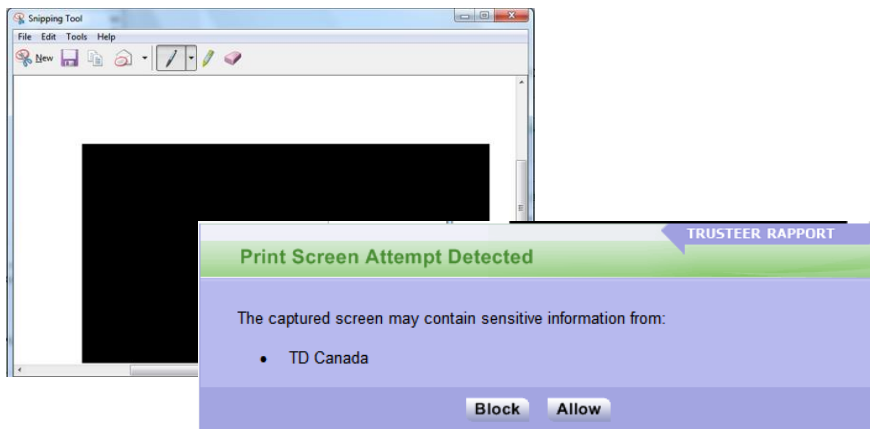
- When you login to some banking sites they offer the ability to download additional free software to reduce the effectiveness of spyware.

– Example: Trusteer is used by a number of Canadian banks.



– (Among other things) this software can prevent spyware from making screen grabs of sensitive banking information when you are at an affiliated financial institution.

Using Anti-Spyware Software: Attempted Automatic Screen Grab Attempts



Protecting Against Spyware

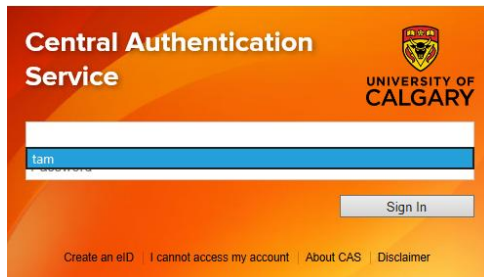
- Some anti-virus programs have begun to expand their services to protect against spyware.
- However there are programs that are dedicated solely to protecting against spyware.
- Some examples:
 - Ad Aware: www.lavasoft.com
 - Spy Sweeper: www.webroot.com
 - Spybot: www.spybot.com
- Similar to an anti-virus program you should *update your anti-spyware program and the spyware definitions* on a regular basis.

Keystroke Loggers

- A specialized form of spyware
- Record some or all of the information entered on a keyboard.
- They may be used for fairly legitimate purposes:
 - Trouble shooting errors
 - Monitoring and evaluating employee performance
 - Crime prevention
- A keystroke logger can be hardware or software based.
- Keystroke loggers can also be a form of spyware that was unknowingly installed.

Preventing/Mitigating The Effect Of Keystroke Loggers

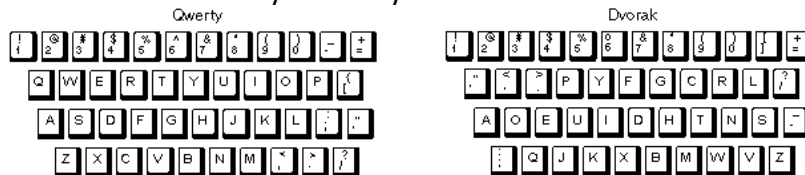
- Install an anti-spyware program.
- Get a firewall: monitors and controls traffic coming into or out of your network
- Minimize the typing of sensitive information with automatic form fillers:



- Use one-time passwords or change your passwords frequently.

Preventing/Mitigating The Effect Of Keystroke Loggers (2)

- Use an alternative keyboard layout:



- Fully custom keyboard layouts can be created using tools like the Microsoft Keyboard Layout Creator.

Preventing/Mitigating The Effect Of Keystroke Loggers (3)

- Using low tech methods can also be fairly effective for some keystroke loggers by 'scrambling' the text entered or by minimizing (or avoiding altogether) the amount of text actually *typed in*.

Preventing/Mitigating The Effect Of Keystroke Loggers (4)

- Two step authentication
 - Password
 - One time code

Other Electronic Counter-Measures Against Malware

- Defensive measures discussed thus far:
 - Getting a good anti-virus program
 - Getting a good anti-spyware program
- Update your operating system (not only for Windows) and key software (e.g., web browsers and programs that run into conjunction with them such as programs that play videos, email readers, MS-Office).
 - Some forms of Malware take advantage of vulnerabilities in the operating system and anti-virus programs and anti-spyware programs are ineffective against them e.g., the Sasser Worm (2004).
 - Updates for Windows and other programs may not only fix bugs and add new features but can also patch these security vulnerabilities.
- Get a firewall (and turn it on/configure the security settings).
 - Software firewalls may get turned off (consider a hardware firewall)

Non-Electronic Based Defenses

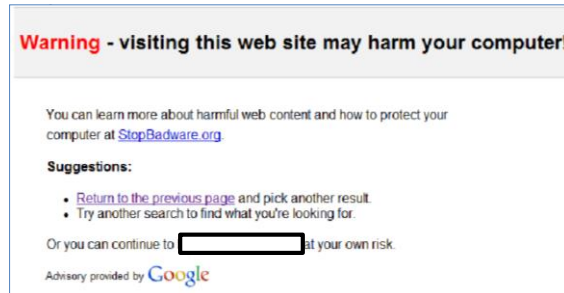
- (Note this list is far from comprehensive).
- Be cautious of all email attachments.
- Be cautious going to unfamiliar websites.
 - Some security programs (e.g., McAfee) and web sites evaluate other websites.

The screenshot shows search results for the term 'warez'. The results include:

- WareZClient.com - Home of WareZ 3**: Copyright © 1994-2006 Neoteric Ltd. All Rights Reserved. WareZ, WareZ P2P, WareZ PRO and the "WZ" Symbol are trademarks of Neoteric Ltd. www.warezclients.com - 10k - [Cached](#) - [Similar pages](#)
- Katz Downloads**: 17 Mar 2009 ... App, ACDSee Photo Manager 10.0.243, Today, 4WareZ-Warez ... Game, Watchmen: The End Is High (2009), Today, 4WareZ-Porn ... [Cached](#) - [Similar pages](#)
- WareZ Oracle Downloads**: RapidShare, MegaUpload and EasyShare download search engine for Games, Software, TV Episodes, Movies, Music, eBooks and more. www.warezoracle.com - 20k - [Cached](#) - [Similar pages](#)
- What is warez? - a definition from Whatis.com - see also wares...**: 14 May 2002 ... WareZ (pronounced as though spelled) ... (Use of warez software is also illegal and may result in a jail sentence) ... search.pro-market.net/techTarget.com/Definition0_servlet_0_servlet_13338_00.html - 59k - [Cached](#) - [Similar pages](#)
- Finsdown Free Full Downloads, Rapidshare, WareZ Download...**: Finsdown Net Full Downloads - Full Version Downloads, Rapidshare Links. finsdown.net - 107k - [Cached](#) - [Similar pages](#)
- warez**: **warez**: n. Widely used in cracker subcultures to denote cracked version of commercial software. ... See **warez** @Ooz, counter, leech, elite ... cwb.org/jargon/html/W/warez.html - 3k - [Cached](#) - [Similar pages](#)
- DDLSpot.com - Your #1 Spot for Full Version WareZ Downloads!**: 16 Mar 2009 ... We provide direct downloads to games, software, movies, mp3, tv shows, and many more downloads for free. www.ddlspot.com/ - [Similar pages](#)

Non-Electronic Based Defenses (2)

- Some search engines (e.g., Google) may block access to sites that may



From www.codinghorror.com

Non-Electronic Based Defenses (3)

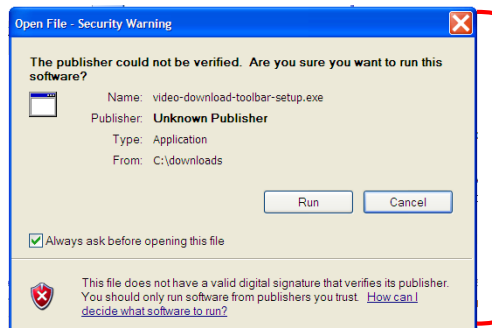
- Only download software from sites that you are familiar with or ones that have a good reputation.
- Alternatively look for software reviewed from reputable sites
 - e.g., www.tomshardware.com, www.pcmag.com
 - These sites may or may not provide direct downloads but at least you will have the names of programs that you can then search for.

Non-Electronic Based Defenses (4)

- Some types of files are riskier than others.
- One way of determining the risk level is to examine the file suffix / file extension (furthest on the right and follows the period in the name of the file).
- Files with the following extensions are dangerous to download: .exe, .pif, and .scr (source: www.microsoft.com)
- Lower risk file types: .txt, .bmp, .jpg and .gif
- Some viruses use files with two extensions to make dangerous files look like safe files e.g., Document.txt.exe or Photos.jpg.exe
 - (This is similar to how “.doc” files can be disguised to appear as “.docx” documents (VBA macro programming section).
- A more complete list:
 - <https://technet.microsoft.com/en-us/library/cc179163%28v=office.14%29.aspx>

Non-Electronic Based Defenses (4)

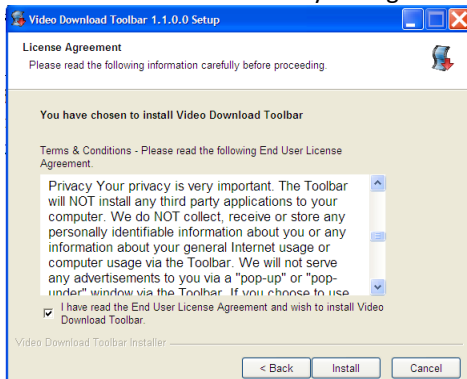
- When you install the program check the publisher information.
 - Installing software from known publishers increases your risk.
 - The identity of ‘known’ publishers is electronically certified by companies such as VeriSign.



Example software with an 'unknown' publisher (but this particular example isn't necessarily malware).

Non-Electronic Based Defenses (5)

- When you install the program read the Terms of Use.
 - Sometimes buried in the text is an implicit agreement to include additional programs or features along with the program that you are installing.
 - Some of these 'extras' may be regarded as Spyware.



An example license agreement for the "terms of use" for the software. (This example isn't necessarily malware).

Non-Electronic Based Defenses (6)

- When you install the program pay attention to the extra 'add-ons'.
 - This is a program that tries to install itself when you are installing another program.
 - Some may be legitimate programs.
 - Others may be more sketchy.
- Some newer browsers may block third party add-on software

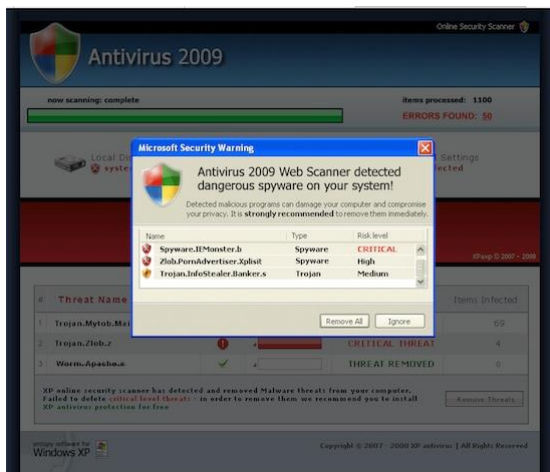
Where To Get Your Software?

↑
More safe

- Direct from the vendor (make sure you go to the right website or even use physical media – yes there is an advantage to getting CD/DVD)
- Getting software from an official ‘app-type store’ (some stores are safer than others)
- Go to sites recommended by reputable sources e.g. computer magazines (PCMag)
- The general Internet (e.g. you find via a search website)
- ‘Pirate’ websites: ‘torrents’, ‘warez’ (offer ‘cracked’ commercial software)

↓
Less safe

Is This A Trap? How To Avoid?



A popup comes up looking like something legitimate from Windows. How do you avoid installing malware when you see this window?

From:
www.thegeekreview.com

Scareware

- In-and-of itself this is not necessarily a malicious program.
- It's an authentic looking message giving you a fake warning about problems with your computer.
 - Virus infection
 - Damaged operating system files slowing down your computer



From: <http://www.symantec.com>

Scareware (2)

Typically pops up while browsing a web site.

- It may simply be an elaborate ruse to get people to try their product.
- In other cases trying to remove a problem that doesn't exist may actually create new problems:
 - Malware infection
 - Credit card theft
- Try closing your browser or even rebooting your computer and see if the messages persist.
- Examine the messages carefully, are they originating from a security program currently installed on your computer?
 - E.g., "Tam secureguard sez' u r infected"
 - Try running your own anti-virus software and see if the "security software" shows up as an infection.

Information On Avoiding Scareware Pitfalls

- Example tips (From Microsoft):
 - Promises of money for little or no effort.
 - Deals that sound too good to be true.
 - Alarmist messages and threats of account closures.
 - Check the return email address
 - Don't click on the links provided to 'fix' the problem
 - Use common sense e.g., would a computer tech administrator require personal information to 'verify your email account information'
 - Requests to donate to a charitable organization after a disaster that has been in the news.
 - Just donate directly via the website rather than using the email
 - Bad grammar and misspellings.
- For more information:
 - <http://www.microsoft.com/security/pc-security/antivirus-rogue.aspx>

Scammers Are Annoying But...

- ...it's probably best to avoid confrontations:
 - <http://globalnews.ca/news/1444283/calgary-couple-harassed-over-phoney-lottery-scam/>

Some Security Issues While Browsing The Web

- Incorrect web site names
- Browser hijacking
- Storing financial information
- Saving previously entered data

Incorrect Website Names



www.amazn.com

Visa number: 123 456

....

Person behind the fake website



Visa number:

123 456

Think this could never happen to you?

- <http://www.ucal.gary.ca/>
- Also: sometimes incomplete web addresses are displayed on mobiles

Incorrect Website Names

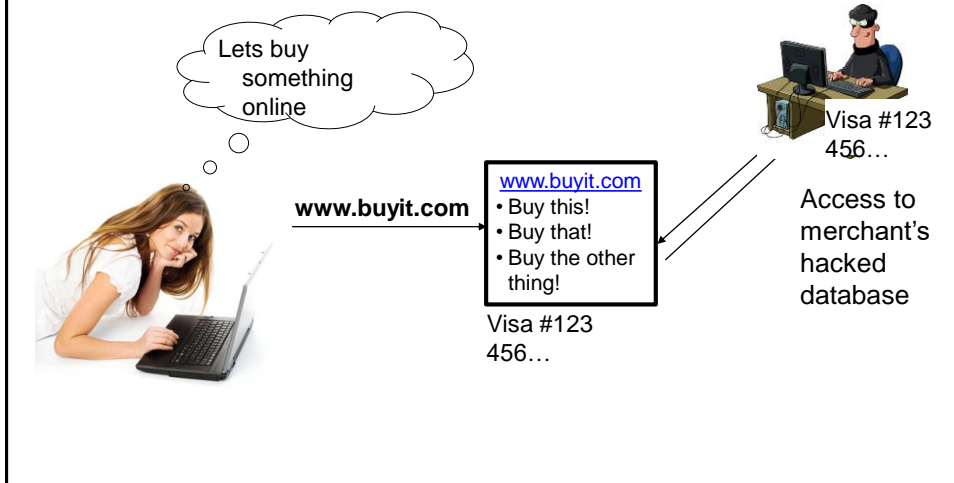
- How to mitigate
- Use a reputable search engine to find the desired website
- “Favorite” or “bookmark” websites and then access the website using this way rather than typing it manually each time.
- Social media can be far from the safest source:
 - <http://money.cnn.com/2017/11/24/technology/black-friday-cyber-monday-shopping-scams/index.html>
- Sometimes a source that you viewed as reputable may make mistakes
 - <https://www.nytimes.com/2017/09/20/business/equifax-fake-website.html>

Browser Hijacking

- A program that takes over your web browser:
 - Changes your default home page
 - Changes your favorites/bookmarks in your browser
 - Causes a storm of pop-up windows to appear
 - Redirects the browser to certain web pages
 - Redirects the browser away from certain web pages (e.g., websites run by companies that product anti-virus software)
- Common sources
 - ‘Free’ software (Trojan)
 - Email attachments
 - Drive-by downloads (covered earlier)

Storing Financial Information

- Even if you enter your information at the correct web site the convenience must be balanced out vs. security concerns:

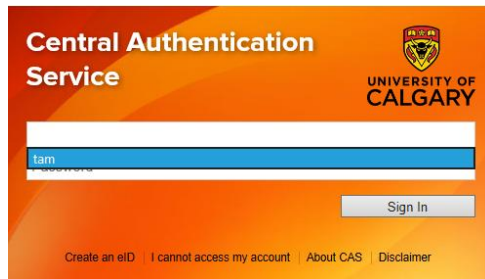


Storing Financial Information (2)

- Balance the convenience of having this information stored with the merchant (so you don't have fill it) and the additional security (foiling spyware such as keystroke loggers) vs. the probability of having it stolen from the merchant.
- Consider:
 - The size of the merchant (large with the resources to spend money on security vs. a tiny home business).
 - The merchant's reputation and history (keep in mind that quite often merchants legally don't have to disclose security breaches).
 - Any security measures that they care to describe (specific measures, e.g., 128 bit encryption, rather than just vague guarantees about protecting your information).

Saving Previously Entered Information

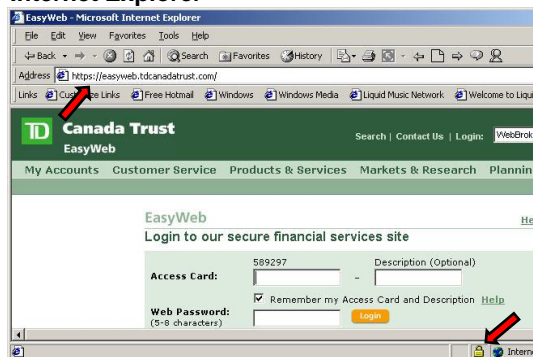
- Even storing information on your own computer must balance convenience against *some* security concerns.



Transmitting Information On The Internet

- Many protocols transmit packets in an unencrypted format.
 - Email
 - Http
- Indicators that a web page employs encryption

Internet Explorer



General

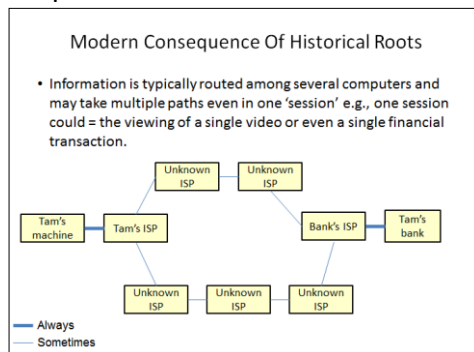


What Is Encryption?

- “Scrambling” information sent across a network (or the Internet)
- Example:
 - Original message: MARY HAD A LITTLE LAMB
 - Encrypted message: LZQX GZC Z KHSSKD KZLA
- The sending computer encrypts the information
- The encrypted information is sent along the network/Internet
- The receiving computer decrypts the information

Why Bother With Encryption?

- I “trust” the website that I am dealing with!
- Keep in mind how the Internet is set up:



- Strong encryption means that the administrators of the intermediate computers cannot view the information

Choosing A Good Password

- Even with the best encryption, if the password is weak a brute force approach can 'crack' your security.
 - Because computers of today perform math quickly and a brute force approach is just mathematically going through possible combinations a poorly chosen password can eventually be determined.
 - E.g. 3 binary digit password and "brute force" hack
 - 000
 - 001
 - 010
 - 011
 - 100
 - 101
 - 110
 - 111
 - 2 raised to the number of bits = number of combinations

Choosing A Good Password (2)

- The more bits used, the harder it is to guess ('crack') the password
- $2^1 = 2$ combinations
- $2^2 = 4$ combinations
- $2^3 = 8$ combinations
- ...
- $2^{24} \sim 16$ million combinations
- $2^{32} \sim 4$ billion combinations

Choosing A Good Password (3)

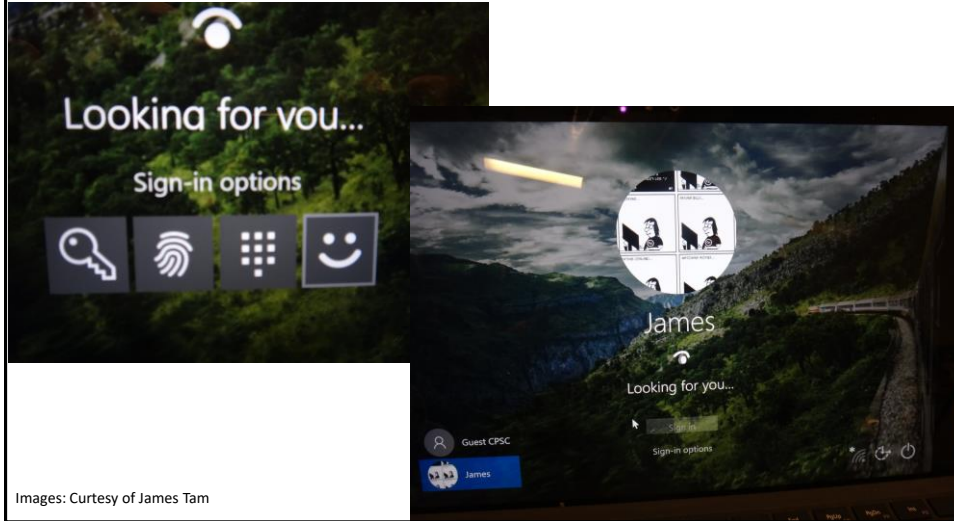
- Using different characters makes it even harder to guess a password
 - E.g. same case alpha
 - Using a single alpha (lower case) = 26 combinations
 - Using two alpha (lower case) = 26 x 26 combinations
 - E.g. mixed case alpha
 - Using a single alpha (upper and lower case) = 52 combinations
 - E.g. mixed case alpha and digits
 - Using a single alpha (52 mixed alpha plus 10 digits) = 62 combinations

Guides For Password Security

- Things to avoid in passwords
 - Never choose something of direct personal meaning to yourself that someone can guess
 - Name, birthdate, address, pet's name etc.
- Things to guide your choice of a password
 - Avoid using dictionary words (that part of the password can be easily guessed)
 - Use a mix of alpha (mix case), numeric, "special characters"
 - E.g. Marieieie-is_mEye:-)BaE
- But you may have heard that the password creation rule of thumb (e.g. use special characters) is 'bad'
 - Compare: 'Ab&9' vs.
'eiejknienjneikeijhvjkkjkjeudhhdjhuieienjhee'
 - Better: 'Akieiek_9DUEb&9'

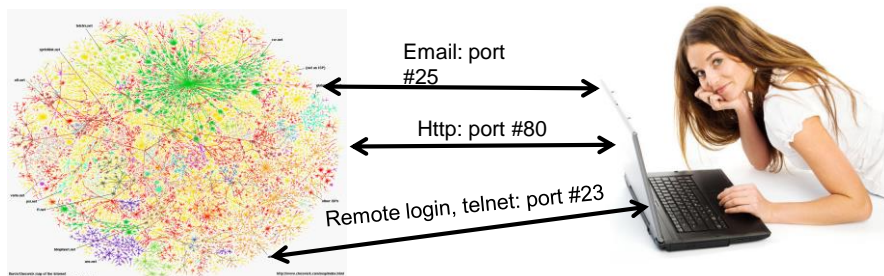
Password Alternatives

- Finger print and facial recognition



Interacting With Parts Of The Internet

- The World Wide Web (WWW) is only one part of the Internet (albeit a very popular part).
- There are other parts (e.g., file transfers, email etc.)
- Your computer interacts with these parts of the Internet through that computer's 'logical ports' (numbers)



Evaluating The Effectiveness Of Your Firewall

- Firewalls may help to secure your computer by blocking ports with security problems.
 - General rule of thumb: if you don't use a port then don't open it for access with your firewall.
 - E.g. Port 25 is frequently used to send spam mail
- If you are unsure of how to configure your firewall:
 - Use the default or recommended configuration
 - Use a trusted source to evaluate the security of your firewall
 - Example "Shields up"
 - <https://www.grc.com/x/ne.dll?bh0bkyd2>
 - Some firewalls do all or most of the configuration of the ports for you (e.g., Norton).

General Ways Of Increasing Your Computer Security

- Install an anti-virus program from a reputable company.
 - Update the definitions on a regular basis.
- Install an anti-spyware program from a reputable company.
 - Update the definitions on a regular basis.
- Add a firewall.
 - Make sure that it's properly configured.
 - (Don't use the default password)
- Update your operating system and programs on a regular basis.
 - The updates not only provide bug/error fixes but may also patch up security flaws.

General Ways Of Increasing Your Computer Security (2)

- If your computer appears to be acting abnormal then you may try scanning for suspicious processes.
- Use utilities like the Task Manager to see what processes are running and if unfamiliar ones are taking up most of your processor time.

A General Checklist

Checklist: Protect Your Security

Think you're pretty up to date on your security practices?
Let's see for sure with our handy checklist.

- Install current anti-virus software, like McAfee AntiVirus
- Download additional security software such as Rapport
- Make sure you have the latest supported web browser
- Check your credit report once a year
- Set up a passcode to unlock your mobile phone screen
- Keep your PIN numbers and passwords to yourself
- Ignore unsolicited emails that ask for your personal info
- Change your default wireless router password
- Look for the lock icon in the Address Bar before entering personal info into a website
- Limit the amount of personal info you share on social networking sites

See how you did ▶

Source: <http://www.scotiabank.com/>

Things To Do If Your Computer Appears To Be Running 'Funny'



1. Update security software
2. Update virus definitions
3. Run security software (Complete steps 1 & 2) **before** #3
4. Start up the Task manager and look for unusual processes running and/or ones that are taking up many system resources
5. Look at installed programs on control panel, sort by date and look at programs installed around or after you noticed things going weird
6. Look at browser "extensions" (Microsoft)/"add-ons" (Firefox)/"plug-ins" (Chrome)

(Of course your problem could be caused by faulty hardware or software).

Microsoft Browser 'Extensions'

Extensions in Microsoft Edge

To find an extension and add it to your browser:

- ① Open **Microsoft Edge**  and select **Settings and more**  > **Extensions** > **Get extensions from Microsoft Store**. (If you don't see Extensions on the menu, note that you must have the Windows 10 Anniversary Update before you can use extensions.)
- ② Select the extension you want, and select **Free** to install it.
- ③ Once the installation is complete, switch back to Microsoft Edge.
- ④ Read the notification about what the extension will be allowed to do, and select **Turn on**.

 Help from Microsoft

Was this helpful?  

Privacy And The Internet

- Is it a big deal?
- Think of all the public figures whose past online activity have come back to haunt them.
- Here's a few extreme cases that effected people who weren't public figures:
 - Unrepentant on Facebook? Expect jail time (from CNN:
 - <http://www.cnn.com/2008/CRIME/07/18/facebook.evidence.ap/index.html>
 - Teacher arrested for pro-Columbine blog post
 - <http://www.cnn.com/2007/US/law/12/04/blog.arrest.ap/index.html>
- If you're not a public figure then is privacy and information listed online important to you?
 - Planning to ever apply for a job that is important to you?
 - <http://www.management-issues.com/2006/10/27/research/your-digital-dirt-can-come-back-to-haunt-you.asp>
 - Ever planning to go on a date?

Privacy And The Internet (2)

- The Internet (and especially the web) is not a private place.
- What you (or someone else) posts there is not only viewable by the world at large but is likely to remain available (in some form) even should the offending information be removed.
 - E.g. 1, search engines often save old information about web sites
 - E.g. 2, there are specific web sites that provide archived versions of the web that go back many years.
 - E.g. 3, the terms of use for some web sites imply that any content (text, pictures, videos) uploaded to their site by users may be available indefinitely even if the user later removes the content from the site.

Posting Information

- While providing and sharing personal details is one of the main benefits of social networking sites such as Facebook, MySpace, Twitter etc. this must be balanced out vs. the potential costs of providing too much information.
 - Providing too much information about your personal details may make you a target of identity theft.
 - It may also make it easier for direct marketers to target their wares (because they know your likes and dislikes).
 - There is also the possibility of becoming the target of crime.
- This isn't to say that you should never post anything online, just *think about the potential consequences*.
- Also pay attention to *what other people post about you!*
 - E.g., "Tagged" online images of you.
 - But reverse image searches are now possible (not tagged)

Posting Information (2)

- The more information that you post about yourself the more vulnerable that you may become.
 - "The sinister side of social networking", CNN:
<http://www.cnn.com/2007/WORLD/europe/09/07/ww.sinistersocial/index.html>
- Posting one of the following in isolation may not be a problem but the more pieces of information that are posted the more problems that may arise.
 - Information that you should be less willing to give out to everyone:
 - Your financial information e.g., Social Insurance number, credit card and bank information (obvious?).
 - Your address and/or phone numbers.
 - Your full name (you might want to check what information can someone get from this with even a simple web search).

Posting Information (3)

- (Potentially sensitive information that is less obvious):
 - “Entertaining” pictures of yourself.
 - Your likes and dislikes e.g., favorite color, make and model of your first car, your pet’s name etc.
 - Information about yourself that isn’t financially related or providing contact information e.g., your pet’s name, mother’s maiden name
 - Your full date of birth (or partial birth date along with your age).
 - Status information e.g., announcing online that you will be out of town for a period of time while at the same time there’s clues (direct or indirect) about where you live.

Online Privacy: Considerations

- Your “real” friends have as much personal information about you online that they have in the real world.
 - What’s the problem with posting personal details?
- Don’t forget though that the web site operator also has access to this information
 - Providing this information to your online friends may be the same as giving it the website administrators.
 - Read their terms of use because they may be allowed to share this information to other companies)
 - Or ‘app’ or websites that you ‘like’ may be able to access your personal details

Online Privacy: Considerations (2)

- Keep in mind that your friends may also be subject to identity theft.
 - Did your real-world friend actually set up the account and is the one who is currently using it or does someone else have access to it).
 - Your friend could get 'hacked'.
 - Keep these two points in mind as you post (even if you set 'friend's only' access to your online account
 - Finally even if the account of your online friend is indeed accessed only be your friend and if you think that your friend may never be hacked (big if) consider your friend's security settings
 - In the past Facebook would allow for insecure ([http](http://)) login
 - Not encrypted!
 - It was only after a few years of operation that logins can only be done securely ([https](https://))

After This Section You Should Now Know

- What is malware
 - What are some common categories of malware
 - How do the different forms of malware get onto your computer
 - What are the consequences of having a malware infection on your computer
 - How to protect against malware
- Electronic and non-electronic defensive measures against malware
- What is scareware and how it can be a security threat
- What are some common web-based security issues and how to mitigate some of them
- What is a browser cookie
- What are the different types of cookies and how do they differ

After This Section You Should Now Know (2)

- What is a logical port and how do firewalls increase security by closing ports
- What is encryption and how does it tie into security
- General ways of increasing the security of your computer
- The importance of protecting your online privacy
- What is the potential cost of having your personal information online
- How to minimize the risks of providing information online