

Computer Security

A brief and practical guide to computer and Internet security

Why Security Is Important: News Stories & Media Links

- <https://www.theregister.co.uk/security/>
- <https://catless.ncl.ac.uk/Risks/>
- <https://krebsonsecurity.com/>
- <https://www.ctvnews.ca/canada/credit-card-skimmers-found-at-vancouver-transit-stations-1.4010396>
- <https://calgary.ctvnews.ca/video?playlistId=1.4070367>
- <https://www.ctvnews.ca/canada/three-digital-scams-to-watch-out-for-1.3916802>
- <https://globalnews.ca/news/4110785/facebook-data-scandal-payments-industry-retailers-canada/>
- <https://globalnews.ca/news/3984952/peterborough-police-warn-of-death-threat-email-scam/>
- <https://globalnews.ca/news/4353447/dont-be-fooled-by-the-password-email-scam/>
- https://www.consumer.equifax.ca/personal/education/identity/5-traveling-habits-that-put-you-at-risk-for-identity-theft?CTID=suitcase&utm_source=360i_facebook&utm_medium=social_article
- <https://globalnews.ca/news/4353684/alberta-health-services-phishing-scam/>

Why Security Is Important: News Stories & Media Links (2)

- <https://www.ctvnews.ca/business/crtc-levies-fines-against-two-companies-under-canada-s-anti-spam-law-1.4010248>
- <https://globalnews.ca/news/4369709/cryptojacking-computer-malware-threat-cryptocurrency>
- <https://www.ctvnews.ca/canada/three-digital-scams-to-watch-out-for-1.3916802>
- <https://globalnews.ca/news/4369709/cryptojacking-computer-malware-threat-cryptocurrency>
- <https://globalnews.ca/news/4238897/bmo-simplii-customers-information/>
- https://www.gamespot.com/gallery/how-to-protect-your-gaming-pc-from-malware/2900-1599/?utm_source=weekly_newsletter&utm_medium=email&utm_campaign=20160510&utm_ee=1HOaudAeIVvgLqdRV+YG8yBcNiqpZ2stzvnzhg4JEiMjKkyTeVZl95Ss7Y6fO3&utm_ts=1518127522278

Test

- You get a file attachment in a message, from which of the following people would you should you open it without precautions and why?



A total stranger



Someone you've only met on the Internet

Colourbox.com



Your best friend

Colourbox.com

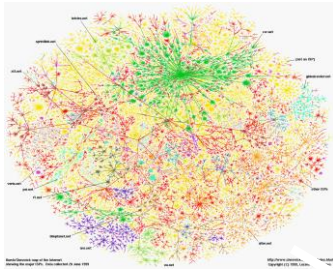


This guy!!!

Bottom Line

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

Guaranteed Electronic Security



Disconnect your
computer/device from
the Internet

Leave your
computer/devices
off all the time

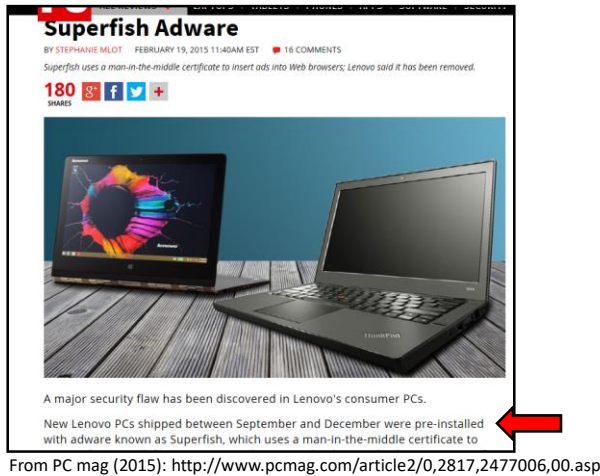
Put your
them all in a
vault (never
use



From: www.colourbox.com

Guaranteed Electronic Security (2)

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



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.
 - **Problems with simple solution #1**:
 - 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>

Guaranteed Electronic Security (4)

- **Problems with simple solution #2:**
 - Viruses (and other malicious problems) **DO** exist for operating systems other than Windows
 - Examples of Mac viruses & security issues:
 - <https://www.macworld.co.uk/feature/mac-software/mac-viruses-list-3668354/>
 - Examples of Linux viruses & security issues:
 - <https://www.techrepublic.com/article/linux-unix-viruses-and-worms-demand-special-attention/>

Guaranteed Electronic Security (5)

- 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.

(New?) Terms Commonly Used In Conjunction With Security

- Hacker
- Hacked computers (or other device)
- Phishing (and the related term Spearphishing)

New Term: 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....

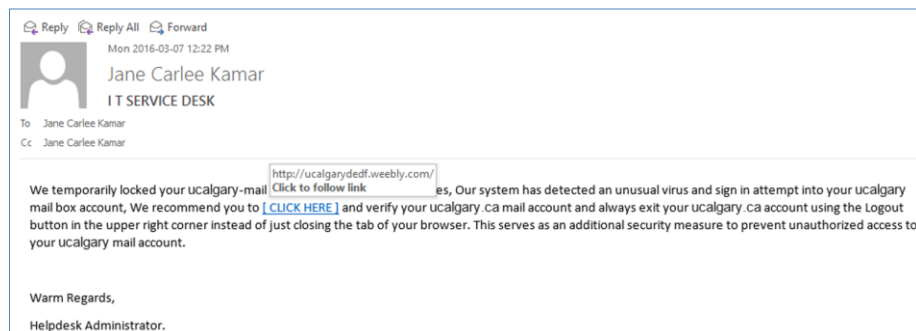
...from the Winston Salem Journal

New Term: “Hacked” Computer System / Device

- 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
- Keep in mind this term is used in popular culture (even by news media outlets) for less serious security issues.


New Term: Phishing

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



Reply Reply All Forward

Mon 2016-03-07 12:22 PM

 Jane Carlee Kamar
IT SERVICE DESK

To: Jane Carlee Kamar
Cc: Jane Carlee Kamar

We temporarily locked your ucalgary-mail [Click to follow link](http://ucalgarydedf.weebly.com/) es, Our system has detected an unusual virus and sign in attempt into your ucalgary mail box account, We recommend you to [CLICK HERE](#) and verify your ucalgary.ca mail account and always exit your ucalgary.ca account using the Logout button in the upper right corner instead of just closing the tab of your browser. This serves as an additional security measure to prevent unauthorized access to your ucalgary mail account.

Warm Regards,
Helpdesk Administrator.

How Many “Fall For” Phishing?

- 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 U of C 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:
 - Would one good login negates several ‘bad’ logins?
 - Why would your ‘login to confirm your account’ make any difference if there were several suspicious or invalid attempts.
- A *slightly* better scam would at least ask you to login and change your password

Slightly Better Phishing Attack

- **New term: “Spear phishing”**¹: 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 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**’ or ‘**web scripts**’).
 - **New term: Drive by download** (getting an electronic infection from just visiting a website).
 - Skeptical? Try going to this web address (don’t worry it’s not a real virus infection)
 - <https://pages.cpsc.ucalgary.ca/~tami/2017/203F/autorun.html>

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

The collage consists of several overlapping browser window screenshots:

- A Facebook page with a "JavaScript Required" error message: "We're sorry, but Facebook doesn't work properly. When you have eliminated the JavaScript, whatever remains must be an empty browser window. Enable JavaScript to see Google Maps."
- A YouTube page with a yellow box saying "A-OK!" and the text "The faculty home page of James Tam".
- A browser window showing a warning: "Detecting if CAS authentication is required..."
- Other browser tabs and address bars are visible, including "https://my.ualgary.ca/" and "https://www.gotinder.com/".

Preventative Measures Against Drive By Downloads

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

The screenshot shows search results for "warez" and "warez client". 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.warezclient.com/ - 15k - Cached - Similar pages
- Katz Downloads**: 17 Mar 2009 ... App, ACDSee Photo Manager 10.0.243, Today, 4Waz-Warez ... Game, Watchmen: The End Is High (2009), Today, 4WareZ-Porn ... [katz.cd/](#) - 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: warez ...**: 14 May 2002 ... WareZ (pronounced as though spelled ... (Use of warez software is also illegal and may result in a jail sentence) ... searchcio-midmarket.techtarget.com/sDefinition0_sid183_gc1213338_00.html - 56k - 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**: 'weɪz'; n. Widely used in cracker subcultures to denote cracked version of commercial softwares. ... See warez d00tz, c0unter, leech, elite ... calb.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

Preventative Measures Against Drive By Downloads (2)

- Some search engines (e.g., Google) may block access to sites that may infect or otherwise harm your computer.


Warning - visiting this web site may harm your computer!

You can learn more about harmful web content and how to protect your computer at StopBadware.org.

Suggestions:

- [Return to the previous page](#) and pick another result.
- Try another search to find what you're looking for.

Or you can continue to at your own risk.

Advisory provided by 

From www.codinghorror.com

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.

New Term: 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 – check is with the Task manager)
 - Increase in network usage (Your ISP may provide ways of letting you know your data usage rate)

New Term: Botnets

- Paraphrased definition from (Norton: an established anti-virus software manufacturer): <https://us.norton.com/internetsecurity-malware-what-is-a-botnet.html>
- A collection of connected computers (‘zombie’) which together can complete various tasks some of which may be for malicious purposes:
 - A distributed-denial-of-service (DDoS) attack when prevents access to targeted websites
 - Sending spam mail
 - Replacing generic Internet banner ads with ones specifically targeted towards you
 - Generating popups that urge you pay for software to remove your computer from the botnet
 - In general using your computer as part of a network to carry out various nefarious tasks

Why Terminology Is Important: News Media And 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.

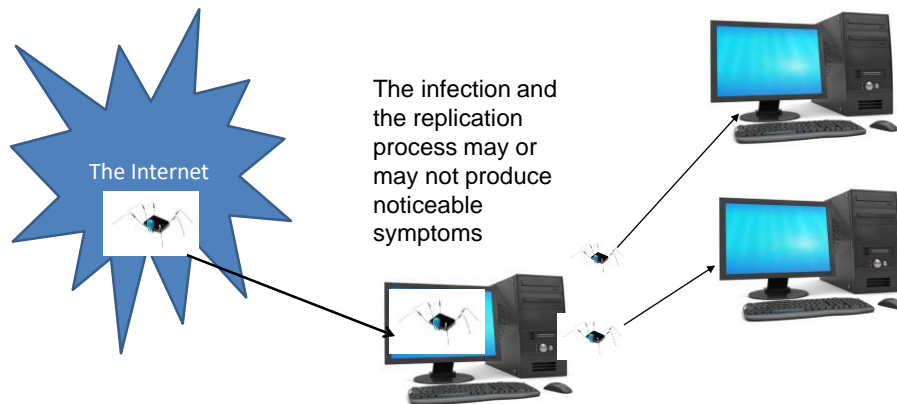
(Exert)

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

- How do the following affect you.
- My financial institution/workplace/university computer system user’s have fallen for a phishing scam?

Computer Virus

- Similar to a biological virus

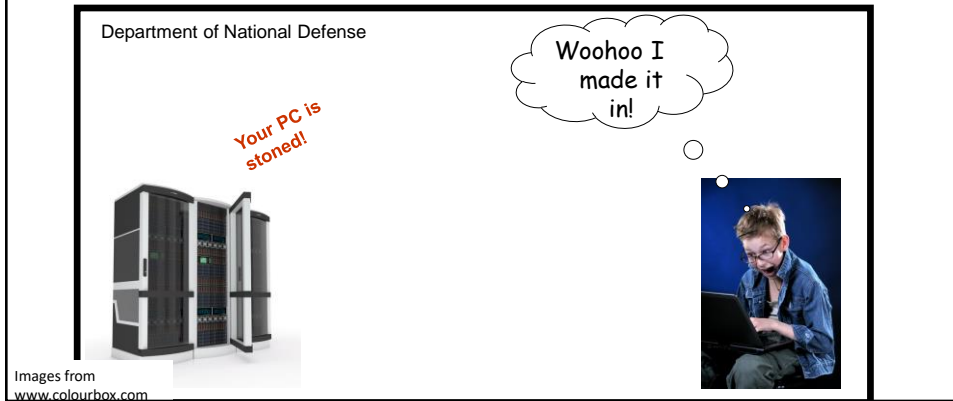


Images from: www.colourbox.com

Computer Virus: Objective

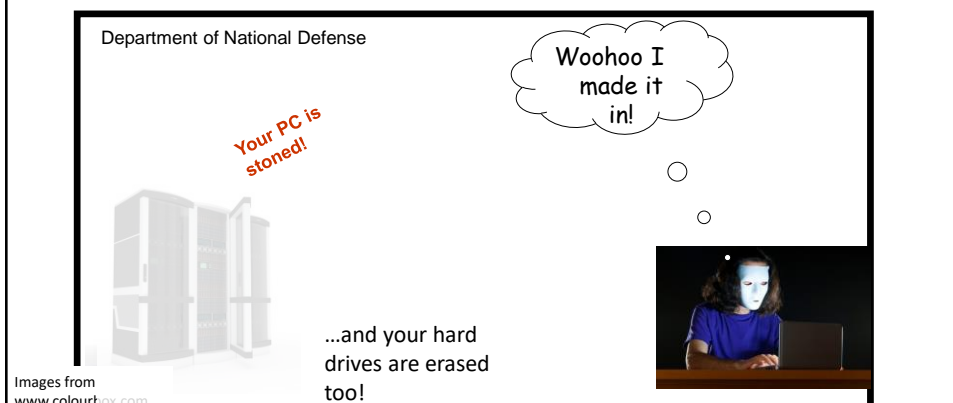
- For early virus writers the goal was simply infiltration of a computer or network.

At most the virus would result in some minor mischief



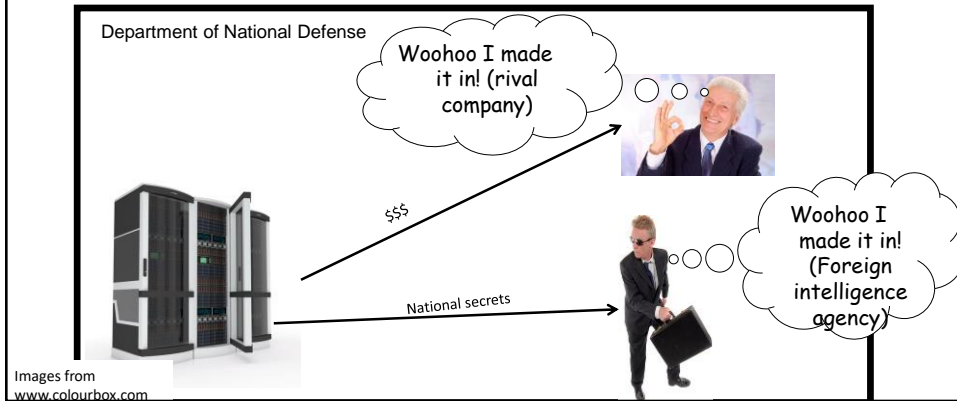
Computer Virus: Objective (2)

- Some viruses were designed to be malicious or were 'mutated' into a malicious version (steals data, damages/deletes files, causes the computer to malfunction etc.)



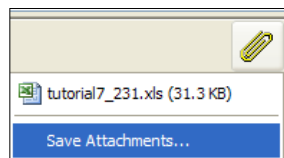
Computer Virus: Objective (4)

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

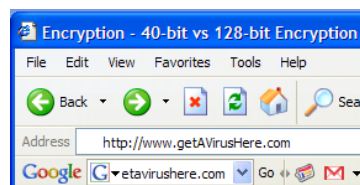


Computer Virus: Spread

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



- Web-based: just going to a website can result in a infection (as mentioned a “drive-by download”).



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

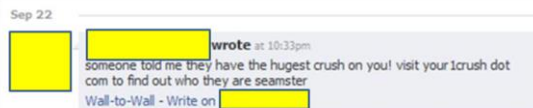
2011	2012	2013
1) Heidi Klum	1) Emma Watson	1) Lily Collins
2) Cameron Diaz	2) Jessica Biel	2) Avril Lavigne
3) Piers Morgan	3) Eva Mendes	3) Sandra Bullock
4) Jessica Biel	4) Selena Gomez	4) Kathy Griffin
5) Katherine Heigl	5) Halle Berry	5) Zoe Saldana
6) Mila Kunis	6) Megan Fox (up from #15!)	6) Katy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

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

Computer Virus (And Other Malicious Programs): 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






Norton Safe Web for Facebook  powered by VeriSign

Your account is currently protected by Norton Auto-Scan. Auto-Scan On Auto-Scan Off

We have examined your Facebook Newsfeed and scanned each link shared within past 24 hours.

Newsfeed scanning complete. 

Links Checked: 30 link(s) shared to you with in past 24 hours.

Norton Secured		19	<div style="width: 63%;"></div>
Safe		9	<div style="width: 30%;"></div>
Caution		0	
Warning		0	
Untested		2	<div style="width: 6.7%;"></div>

Worms

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

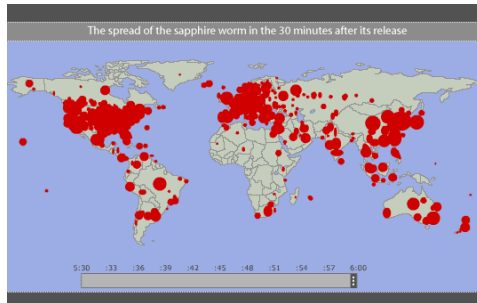


Image and facts from www.pbs.org (Accessed in 2015)

- At it's peak Slammer doubled in size every 8.5 seconds
- Within 10 minutes it infected 90% of the worlds vulnerable host computers

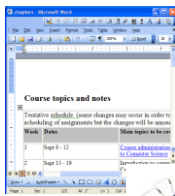
- For detailed information (Symantec anti-virus)
 - http://www.symantec.com/security_response/writeup.jsp?docid=2003-012502-3306-99

Worm: Consequences Of An Infection

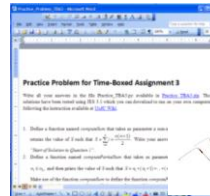
- Worms are designed to automatically spread themselves (ties up computer resources trying to infect other computers).
- They may have other negative effects similar to a virus.
 - “My computer is so slow”
 - My computer is acting ‘funny’

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")`

Macros Viruses

- “Melissa”: Information about an old but ‘successful’ Macro Virus
 - http://www.cnn.com/TECH/computing/9903/29/melissa.02.idg/index.html?_s=PM:TECH
 - <http://www.symantec.com/press/1999/n990329.html>
 - <http://support.microsoft.com/kb/224567>
- Macro viruses aren’t just “ancient history”, take the potential threat seriously!
 - <http://www.symantec.com/avcenter/macro.html>
 - <http://www.microsoft.com/security/portal/threat/encyclopedia/search.aspx?query=Virus>
 - http://ca.norton.com/search?site=nrt_n_en_CA&client=norton&q=macro+virus

Which Document Contains A Macro?

 a	11/1/2015 9:34 PM	Microsoft ...	0 KB
 b	11/1/2015 9:35 PM	Microsoft ...	12 KB
 c	11/1/2015 9:34 PM	Microsoft ...	0 KB
 d	11/1/2015 9:36 PM	Microsoft ...	12 KB
 e	11/1/2015 9:39 PM	Microsoft ...	12 KB

Question: What Is The Security Difference?

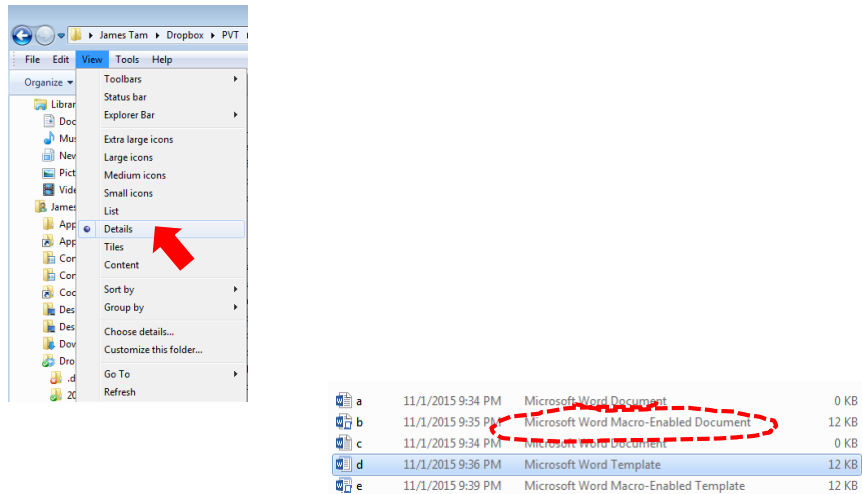
- Opening the following documents:
 - Document.docm
 - Document.docx
 - Document.doc

Types Of Documents That Can Contain Macros (Type 'M')

- You can store the macros that you write for this class this way
 - In a single document 'doc-m' document
- You can also store macros in these documents (not for this class but important to be aware in terms of computer security).
 - Normal 'dot-m' template i.e. "Normal.dotm"
 - Default template used to produce all Word documents (formatting, layout etc.)
 - Custom 'dot-m' template e.g. "histPaper.dotm", "psychPaper.dotm" ...
 - You can override the default by creating your own template documents

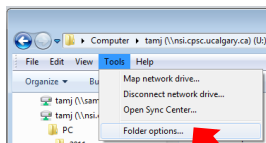
Viewing File Information: Learning What Type Of File Is That Word Document

- View details: select 'view' in a folder

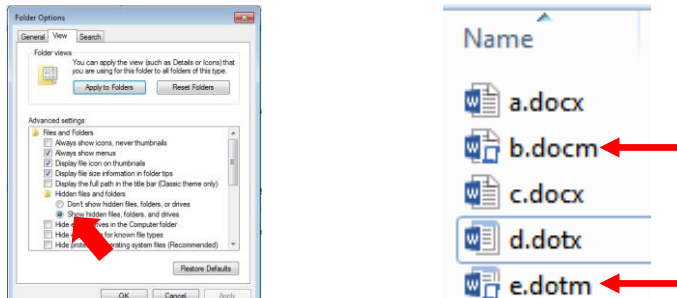


Viewing File Suffixes

- In a folder select: Tools->Folder options



- Under the 'view' tab uncheck 'Hide extensions for known file types'



.DOCX (And .XLSX, .PPTX)

- These types of files cannot have macros attached to them.
 - Reduced capabilities (no macros) but increased security (no macros)
- Question: Are these files with these extensions 100% safe?



Trust me - I'm safe.docx

File name
extensions hidden



Trust me - I'm safe.docx.doc

Enabling the display of
file name extensions

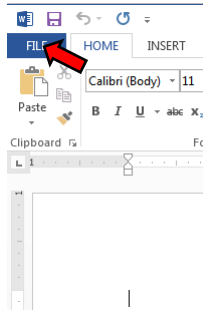
Macros And Security

- Cannot contain macros
 - MS-Office files that really end in 'x' e.g. "docx", "xlsx", "pptx" etc.
 - When you save a document in Office 2007 (or newer) it will in one of these file types.
- May contain macros
 - Template documents, end in dot-m e.g. Normal.dotm
 - Older (Office 97 to 2003) Office documents e.g. "doc", "xls", "ppt" etc.
 - Macro-enabled documents, end in m e.g. "docm", "xlsm", "pptm"

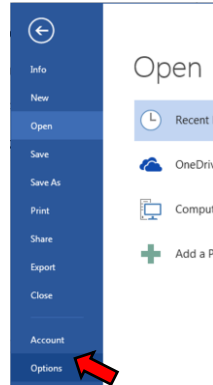
Enabling Macros To Run

- If you can't run macros in MS-office (you see odd error messages) then examine the "Trust Center" settings in Word

1. Select the 'File' ribbon



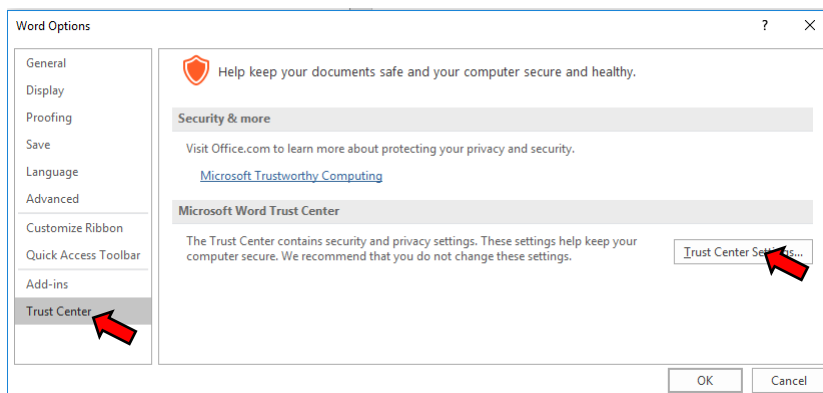
2. Select 'options'



Enabling Macros To Run (2)

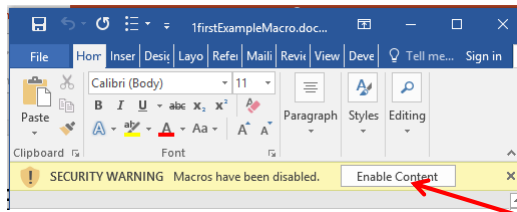
3A) Select "Trust Center"

3B) Select "Trust Center Settings"



Effect: Opening Word Documents

- Using the default setting will disable all macros by default (safer approach) but you can still enable the macros as the document is opened.

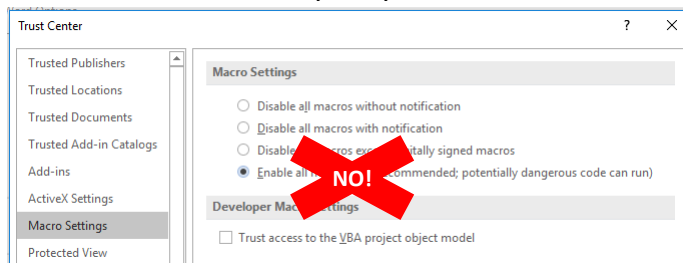


JT's caution

- You should NOT casually select this option for all MS-Word documents
- It's recommended that you ONLY enable macros you have created (or the lecture examples)

Macro Security

- DO NOT take the 'easy' way out



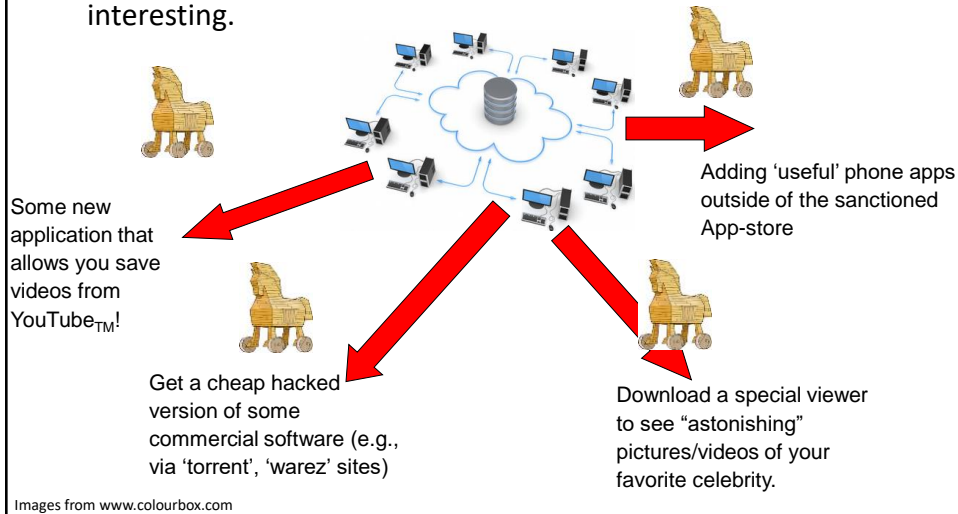
More
secure
↑
↓
Less
secure

For more information:

<http://www.office.microsoft.com/en-us/help/enable-or-disable-macros-in-office-documents-HA010031071.aspx>

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.



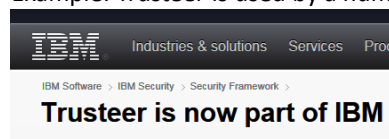
From www.colourbox.com

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)

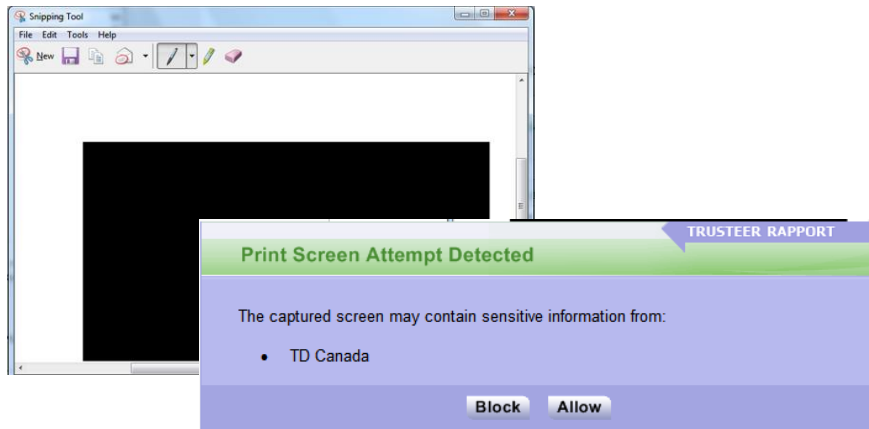
Banking Anti-Spyware Software

- 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

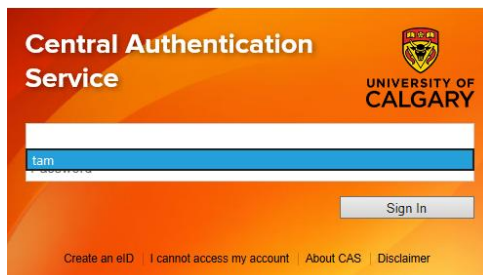
- Some anti-virus programs have begun to expand their services to protect against spyware.
- However there are programs that are dedicated solely to protecting against spyware.
- Some examples:
 - Ad Aware: www.lavasoft.com
 - Spy Sweeper: www.webroot.com
 - Spybot: www.spybot.com
- Similar to an anti-virus 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

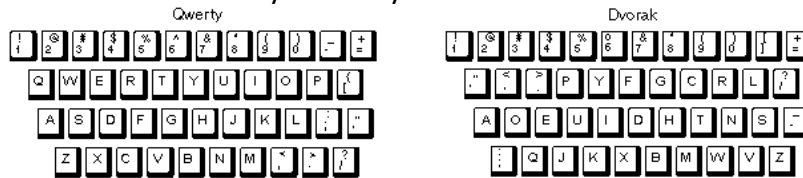
- Install an anti-spyware program.
- Get a sophisticated firewall: monitors and controls traffic coming into or out of your network (more on these later).
- Minimize the typing of sensitive information with automatic form fillers:



The image shows a screenshot of the University of Calgary's Central Authentication Service (CAS) login page. The page has an orange background. At the top left, it says "Central Authentication Service". At the top right, there is the University of Calgary logo and the text "UNIVERSITY OF CALGARY". Below the logo, there is a white input field containing the text "tam". Below the input field is a "Sign In" button. At the bottom of the page, there are links for "Create an eID", "I cannot access my account", "About CAS", and "Disclaimer".

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 (a bit extreme however).

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

Cryptocurrency 'Mining'

- (A greatly simplified explanation):
 - It uses the computing power of a computer to solve complex problems to produce data.
 - The data can be transferred as a currency.
 - Complex verification (is supposed to) make avoid problems of 'faking' the currency.
 - The verification process is also very "processor intensive"
 - Additional details (targeted towards a general audience and generally uses lay terms):
 - <https://www.economist.com/the-economist-explains/2015/01/20/how-bitcoin-mining-works>
 - <https://nationalpost.com/pmnn/news-pmn/canada-news-pmn/what-is-a-digital-currency-and-how-does-cryptocurrency-mining-work>

Cryptocurrency 'Mining' And Security

- On the web
 - Websites may use your computer to mine cryptocurrency when the site is visited.
 - Some websites pay their costs and generate revenue by using visitor's computers during the mining process instead of placing advertisements on their site.
 - Other websites may mine visitor's computers without notice.
- Malware
 - Malicious programs that are installed on your computer may use your computer to mine currency.
 - After the computer is infected the mining may occur independent of what websites are visited or even if a web browser is not running at all.
- Blocking Crypto mining software:
 - <https://www.cnet.com/news/scam-websites-are-using-that-green-https-padlock-to-fool-you/>

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)

Firewalls

- It can come in hardware (e.g. router-firewall combination)
 - This form covers your whole network
- Windows (and MacOS) includes a software firewall
 - This form of firewall can be customized for a particular device (e.g. content filters)
- Many focus on preventing suspicious information (e.g. malware) from downloading into a network or computer
- More advanced features:
 - Examining outgoing information uploaded from a local network or computer to the general Internet
 - Disabling Internet connections (known as 'ports') with known problems (e.g. certain email ports are frequently used by malware that generates spam)

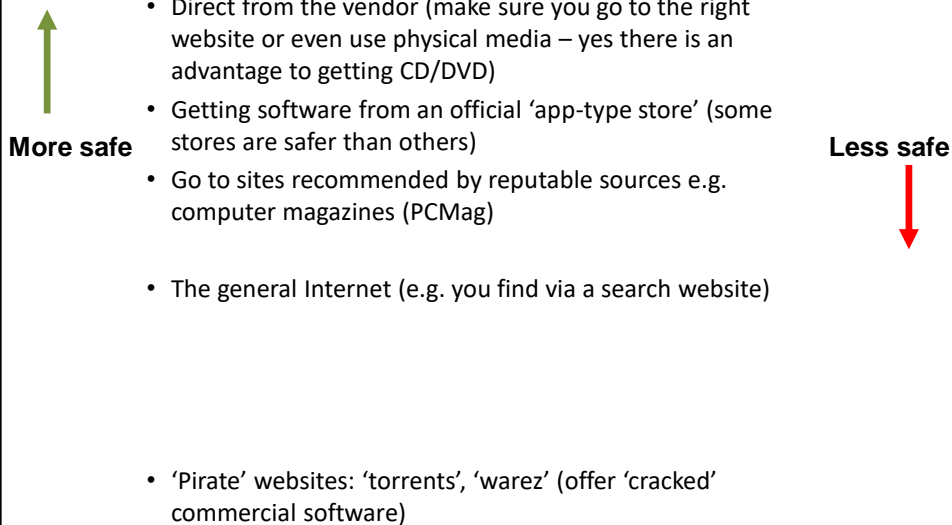
Configuring Your Firewall

- 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 (otherwise it may be used by malicious programs).
 - E.g. Port 25 was used as the default way of sending email, now it is frequently used to send spam mail
- If you are unsure of how to configure your firewall:
 - Use the default or recommended configuration
 - Some firewalls do all or most of the configuration of the ports for you (e.g., Norton).

Downloading And Installing Software

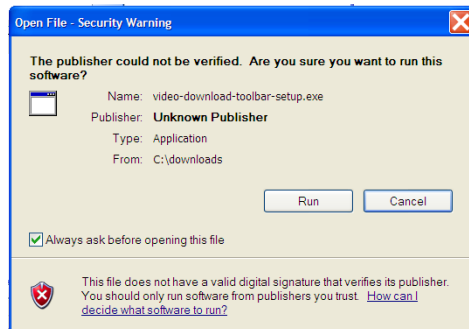
- Only download software from sites that you are familiar with or ones that have a reasonably good reputation e.g. Microsoft.com, apple.com
- Go to the 'App' stores for the company that developing the operating system software:
 - The Microsoft store
 - Apple App store
 - Google play
- Alternatively 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.

Where To Get Your Software?



Check When Installing Software

- When you install the program check the publisher information.
 - Installing software from unknown publishers increases your risk.
 - The identity of ‘known’ publishers is electronically certified¹ by companies such as VeriSign (digital proof that the software actually comes from a particular company).

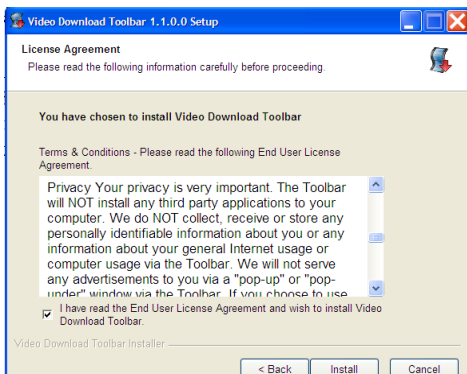


Example software with an ‘unknown’ publisher (but this particular example isn’t necessarily malware).

¹ For more information on digital signatures: <https://acrobat.adobe.com/in/en/sign/capabilities/digital-signatures-faq.html>

Check When Installing Software (2)

- When you install the program at least skim 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).

Check When Installing Software (3)

- 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, installs **(new term) Adware**: software that automatically delivers advertising to your computer) or worse!
- Some newer browsers may block third party add-on software

Ransomware

- This form of attack makes files on your computer inaccessible via encryption until a fee ("ransom") is paid.
- The files can be inaccessible indefinitely although some forms of ransomware may employ additional pressure tactics
 - e.g. "every hour 'x' number of files will be deleted until the ransom is paid".
- The ransomware may be introduced to the system via a Trojan e.g. file attachment, clicking on a link in an email.
- Some ransomware may encrypt a system without a specific action on the part of the user e.g. "Wanna crypt worm"
 - However a security update for Windows did address the security vulnerability
 - <https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/>

Protecting Against/Mitigating The Effects Of Ransomware

- Ransomware may enter a computer system using stolen login credentials and drive by downloads:
 - The same actions taken to avoid falling for phishing scams can help (e.g. be cautious of ‘verifying’ login and other personal information).
 - Avoid suspicious emails links and be cautious of going to unknown websites.
- Backup important files as often as possible (on a device that’s only connected to your computer during the backup).
- Regularly update your operating system (don’t put off those Windows (and other) updates).
- Consider the use of ‘imaging’ software so you can copy the state of your hard drive at a particular point in time (includes configurations and installations that may have been made).

An article by Forbes written for general audiences for dealing with malware: <https://www.forbes.com/sites/waynerash/2020/01/29/how-to-reduce-your-chances-of-getting-hit-with-ransomware/#d4c20dc18754>

Protecting Against/Mitigating The Effects Of Ransomware (2)

- While installing an anti-malware program may sometimes help consider installing a specialized program that is specifically written to detect and counter the behavior of ransomware.
 - These behaviors may range from programs that encrypt or delete files to ones that change the master boot record of the hard drive (where the operating system has been installed)

Portable USB Flash Drives

- Similar to physical health good hygiene practices must be followed.
 - Careless connection of flash drives means that you aren't just vulnerable to malware on that person's computer but any other computers that the flash drive has been connected to.

Is This A Trap? How To Avoid?



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

From: James (credit for the image not for the scareware popup)

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 misspelled words.
- For more information:
 - <http://www.microsoft.com/security/pc-security/antivirus-rogue.aspx>

Side Note: Scammers Are Annoying But...

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

New Term: Encryption

- Unencrypted data (text, images, videos, etc.) can be viewed.
- Encryption processes data so it cannot be viewed until the data is decrypted.
- Many methods (protocols) of transmitting information on the Internet do not encrypt data by default:
 - Email
 - Http (used to be the default for websites)
- Signs that a website uses encrypted connections:
 - https in the web address:



- A lock icon appears in the browser



HTTPS

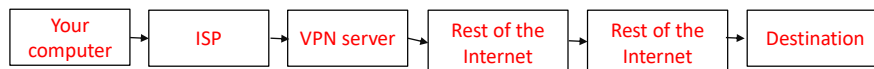
- Browser to browser traffic to a particular website encrypted .
- Potential issues:
 - Other Internet transmissions may not necessarily be encrypted e.g. a separate chat program like Skype (unless the chat program uses it's own encryption).
 - Even though the visual indicators for encryption appear (e.g. lock icon) it's possible that the web traffic is being intercepted and decrypted without any indication to the website visitor:
 - Recall this example: a well known brand of laptops included in their factory software build software that would do this (it was supposed to allowed advertising to be inserted but it could result in other security issues without the laptop user being aware of it).
 - "Man-in-the-middle" attacks. For more information (reputable information source but the link includes a plug for their security software): <https://us.norton.com/internetsecurity-wifi-what-is-a-man-in-the-middle-attack.html>

Not Every Site Employs HTTPS

- Recap of https: an encrypted connection between your computer and the website that employs the https protocol.
 - My connection to a bank <https://www.bankoftam.com> is encrypted.
 - During that same Internet session I check my email on a dating website that uses regular http e.g. <http://www.somdatingwebsite.com> (not a real website) and the information can be viewed by third parties (personal information, contact details, payment information if the site charges).

VPN (Virtual Private Network)

- Encrypts all Internet transmissions (not just your browser).
 - (It can be used with https connections e.g. if you are using a free public hotspot you may be subject to security problems such as Man-in-the-middle type of attacks.
 - Other devices connected to that Wi-Fi hotspot can view ('sniff') information that you have sent out.
 - Even if your information is routed to third party it may not be readable due to the VPN encryption.
 - Keep in mind! VPNs only encrypt information from your computer to the VPN server.
 - After that information may be viewable so it is not a substitute for https.



VPN: More Information

- Explanation:
 - https://headvpn.com/Which_is_better_-_HTTPS_vs_VPN/
 - <https://computer.howstuffworks.com/vpn.htm>
 - <https://www.pcmag.com/article/364072/do-i-need-a-vpn-at-home>
- Review of VPN software:
 - <https://www.pcmag.com/article2/0,2817,2403388,00.asp>
- U of C VPN software: Forte (licensed for student use): see the extra video for getting set up (and it's not just for laptops but licensed for the iPhone and Android).
 - https://ucalgary.service-now.com/it?id=kb_article&sys_id=f7ca400d139962406f3afbb2e144b05f

'Full' End-To-End Encryption

- Although sites such as Facebook only provide https connections you can have chat information fully encrypted from "end-to-end" (only sender and receiver) if you use tools such as "secret conversations" (Facebook tool available only via mobile).
 - One difference between full end-to-end security and https:
 - https: browser to Facebook server encryption (assuming no Man-the-middle attacks computers on the Internet between your computer and the Facebook servers cannot read your information).
 - That means Facebook staff (or others such as: 1) governments that subpoenas Facebook for your information 2) hackers break into Facebook and steal your information) can view transmissions
 - Example article:
 - <https://time.com/4944373/are-your-facebook-messages-private/>

'Full' End-To-End Encryption (2)

- There exist other end-to-end encryption chat programs as well e.g. WhatsApp (owned by Facebook), Telegram, Wickr Me, Signal.
- Of course since the recipient can view messages if you are truly concerned about privacy and security (e.g. "Something coming back to haunt you" in the future) keep in mind that recipient may capture information locally and storage of that information may not be secure e.g. pictures of secure text and files send via secure chat.

Basic Wi-Fi Security: Logging Onto Another Network

- Be cautious when accessing the Internet via free Wi-Fi hotspots!
- First question: is the hotspot actually available in your location (look for physical signage, ask staff).
- Second question: are you actually accessing the free Wi-Fi network or a fake that appears like the actual Wi-Fi connection that you want to access.
 - Similar to fake websites the name of fake Wi-Fi hotspot is spelled very close to the name of the real Wi-Fi hotspot
- Third: avoid logging onto websites where you need to enter or access private information (e.g. bank)

Basic Wi-Fi Security: Logging Onto Another Network (2)

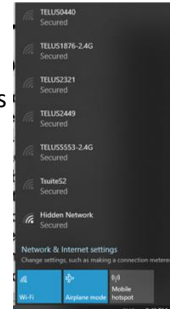
- Fourth: employing a VPN can help prevent others on the network from accessing your information sent to/from your Internet connection.
 - If encryption isn't properly set up on the network then hackers can employ 'packet sniffers' to view the contents of transmissions so the VPN provides encryption.
- Fifth: although convenient don't select an option to connect automatically to the network.

Basic Wi-Fi Security: Configuring Your Home Network

- First: **Change the defaults for the administrator login name, password and even the name of the Wi-Fi network immediately.**
 - Looking at the default Wi-Fi name online may yield the default login information.
- Second: pick a secure password (guidelines to follow).
- Third: apply updates to your router ('flash' the storage device) as they become available.

Basic Wi-Fi Security: Configuring Your Home Network (2)

- Fourth: adds more security but it might be adding unnecessary inconvenience.
 - You can ‘disable’ the broadcasting of the SSID i.e. your router is set up such that the wireless network won’t appear as login option to others.
 - The average person won’t know how to find your wireless network although a more sophisticated user may do so.
- This requires that turn it back when someone with a new device needs to connect to your Wi-Fi network
- Fifth: makes it less convenient to access your home Wi-Fi but makes it harder for someone to find your network.
 - If you do broadcast your SSID you can turn the strength of the Wi-Fi signal to reduce the range of coverage.



Choosing A Good Password

- Even with the best encryption, if the password is weak a brute force approach (brute force = try all combinations) 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. creating a 2 digit password = 100 combinations (more digits used in the password the more difficult it is to guess the actual password)
 - 00
 - 01
 - 02
 - 09
 - ...
 - 99

Choosing A Good Password (2)

- E.g. 3 binary digit password and a 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 (3)

- 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

- This is why, say, 256 bit encryption is better than encryption that uses fewer bits (more combinations)
-

Choosing A Good Password (4)

- Using different characters makes it even harder to guess a password
 - E.g. Using only digits
 - a single digit password = 10 combinations (0- 9)
 - Two digit password = 100 combinations (0-99)
 - E.g. same case alpha
 - Using a single alpha character (lower case) = 26 combinations
 - Using two alpha characters (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

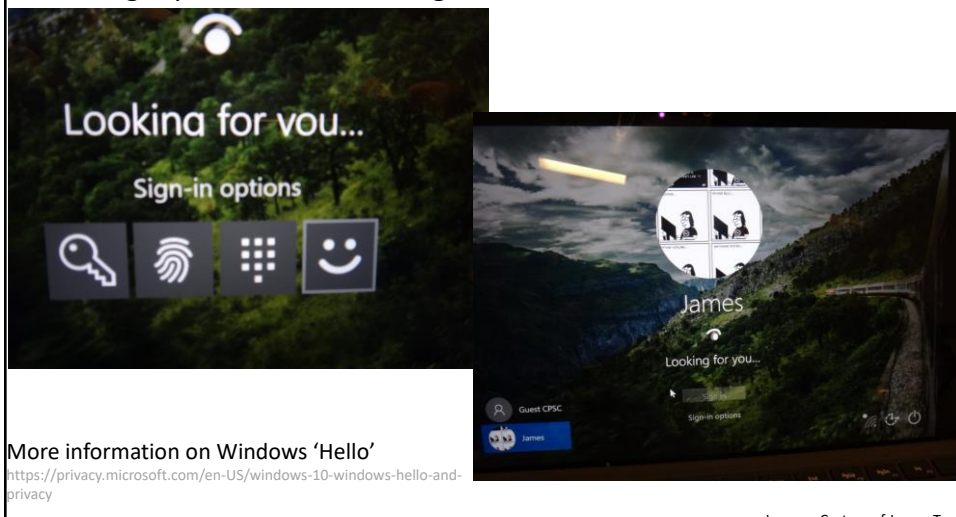
- Things to avoid in passwords
 - Never choose something of direct personal meaning to yourself that someone can guess
 - Name, birthdate, address, pet's name etc.
- Things to guide your choice of a password
 - Avoid using only a dictionary word as a password e.g. 'Sesquipedalianism'
 - Use a mix of alpha (mix case), numeric, "special characters"
 - E.g. My1Bae20Iz300-ZeLdA

Guides For Password Security (2)

- But you may have heard that the password creation rule of thumb (e.g. using special characters) is 'bad' – not in and of itself
 - Compare: 'Ab&9' ($128 \times 128 \times 128 \times 128 = 128^4 \sim 268$ million combinations) vs. "kieiekieie" ($26^{10} \sim 141$ trillion combinations)
 - Short passwords using special characters can be worse than longer passwords that are drawn from one type of character.
 - Better: 'Akieiek_9' = 1,180,591,620,717,411,303,424 or ~ 1 Sextillion combinations

Password Alternatives

- Finger print and facial recognition



Password Alternatives

- Class discussion: what are some of the potential security issues.

Some Symptoms Of A Malware Infection

- Hardware/software changes (note these symptoms may arise by factors other than malware)
 - Computer runs slower (processor, memory, disk usage increase dramatically)
 - Computer malfunctioning (e.g. unexpected crashes)
 - Files are altered (e.g. different default 'open with' program, files have been corrupted)
- The web browser has been altered.
 - Different home/start page
 - The browser is redirected to the different pages
 - New tool bars/adds have appeared
 - Popups unexpectedly appear, sounds play for no apparent reason

Some Symptoms Of A Malware Infection (2)

- An infection may have occurred even if no symptoms are apparent e.g. spyware (if properly written) should “keep a low profile”

Security: Proactive Measures

- 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 (if the previous doesn't protect or protect well from spyware).
 - Update the definitions on a regular basis.
- Add a firewall.
 - Make sure that it's properly configured.
 - (Change the default login and password information)
- Update your operating system and programs on a regular basis.
 - The updates not only provide bug/error fixes but may also patch security flaws.

After An 'Infection': Your Computer Appears To Be Running 'Funny'

1. Update security software
2. Update virus definitions
3. Run security (e.g. anti-virus) 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' (For Your Own Use)

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?  

Firefox Plugins (For Your Own Use)





- From:


- https://support.mozilla.org/en-US/kb/disable-or-remove-add-ons#w_how-to-disable-plugins

How to disable plugins

Beginning with [Firefox version 52](#), support has ended for all NPAPI plugins except for Adobe Flash. See [this compatibility document](#) and [this article](#) for details.

Disabling a plugin will turn it off without removing it:

1. Click the menu button  and choose  Add-ons. The Add-ons Manager tab will open.
2. In the Add-ons Manager tab, select the  Plugins panel.
3. Select the plugin you wish to disable.
4. Select  Never Activate in its drop-down menu.

To re-enable the plugin, find it in the list of Plugins and select  Always Activate in its drop-down menu.

How to uninstall plugins

Most plugins come with their own uninstallation utilities. For help uninstalling some popular plugins, go to [this list of articles](#) and select the article for the plugin you want to uninstall.

- If you are not able to uninstall a plugin, see [Manually uninstalling a plugin](#).

After This Section You Should Now Know

- In terms of computer security, what is meant by the terms ‘hacker’ and a ‘hacked system’ vs a denial of service attack
- How do phishing and spear fishing scams work
- 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
- How do the newer security related threats and issues work: ransomware, cryptocurrency mining
- Electronic and non-electronic defensive measures against malware

After This Section You Should Now Know (2)

- What is scareware and how it can be a security threat
- The different levels of safety/danger when finding software
- What is a logical port and how do firewalls increase security by closing ports
- Security issues related to portable flash drives
- What is encryption and how does it tie into security
- The difference between encrypted and unencrypted information.
 - How different approaches to encryption can reduce security risks
- Examples of Wi-Fi security issues

After This Section You Should Now Know (3)

- Guidelines for choosing a good password
 - How different choices in password can affect computer security (number of combinations)
- How to recognize symptoms of a malware infection and ways of reacting as well as proactively preventing problems

Images

- “Unless otherwise indicated, all images were produced by James Tam

slide 113