

Computer Security

You will learn about some common computerized security threats as well as some ways of minimizing these threats.

James Tam

Test

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



A total stranger



Someone you've only met on the Internet



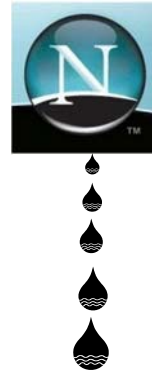
Your best friend



This guy!!!

James Tam

Browsers Are Leaky



- This stems from the origins of the web:
 - Sharing information among researchers
 - Debugging transmission problems

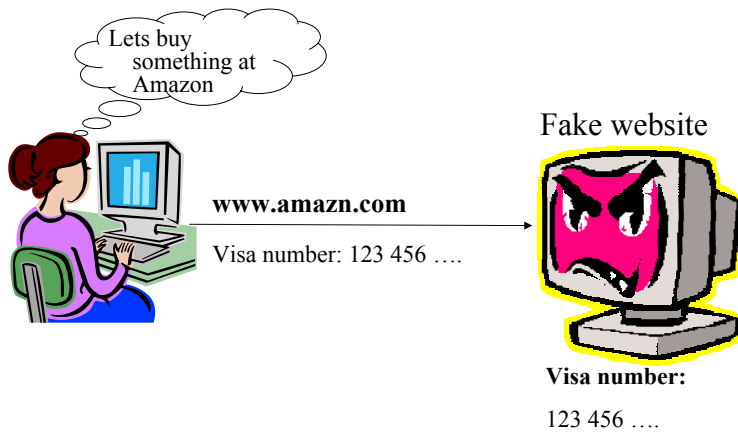
James Tam

Some Security Issues While Browsing The Web

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

James Tam

Incorrect Website Names



James Tam

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
 - Prevents the browser from reaching other pages
- Common sources
 - 'Free' software
 - Email attachments
 - Drive-by downloads

James Tam

Storing Financial Information

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



James Tam

Saving Previously Entered Information

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

Sign On

WARNING: Protect your confidential information!


I agree to SIGN OFF* when I am finished my Web Applications and Portal sessions:

1. **Sign off*** all Web Applications (such as PeopleSoft, Blackboard, Webmail).
2. **Sign off*** from my Portal (My UofC) session.
3. Close all active browser windows before leaving my computer.

* Sign off does **not** mean just closing the open window -- **I must click on the Sign Off link.**

eID:

Password:

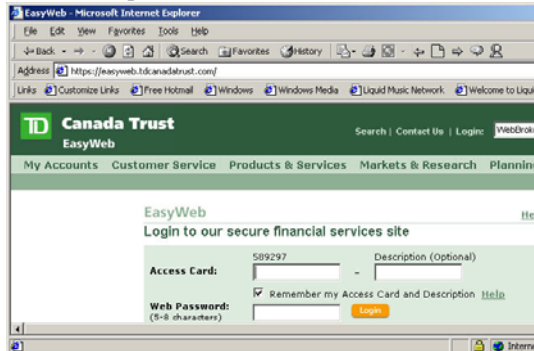
Sign On 

James Tam

Transmitting Information On The Internet

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

Internet Explorer

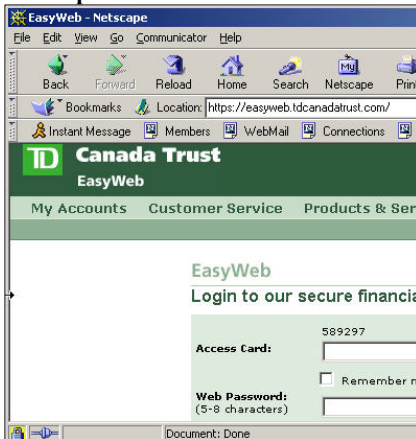


James Tam

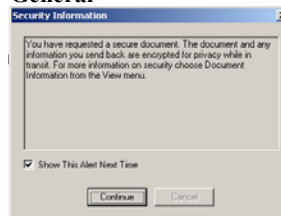
Transmitting Information On The Internet (2)

- Indicators that a web page employs encryption (continued):

Netscape



General



James Tam

Malware (“Malicious Software”)

- A program designed to infiltrate or damage a computer.
- Most of the references to computer viruses are actually references to malware.
- Categories of Malware:
 - Viruses
 - Worms
 - Macro Viruses
 - Trojans / Trojan Horses
 - Spyware

James Tam

Viruses

- Similar to a biological virus

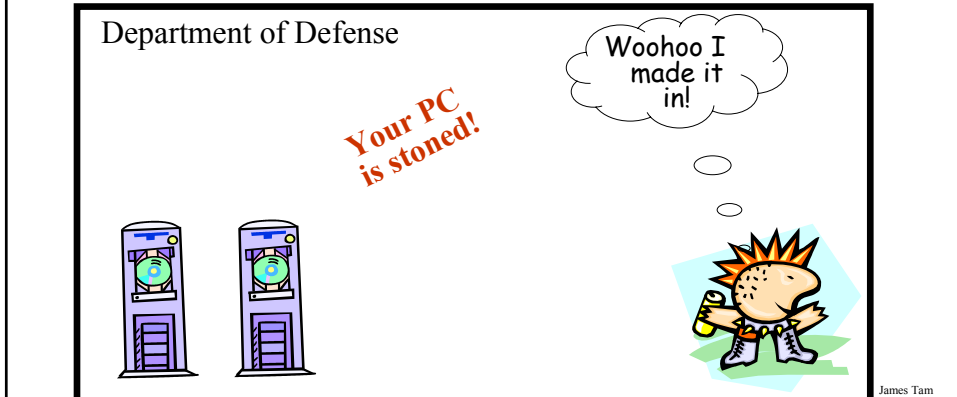


The infection and the replication process may produce symptoms

James Tam

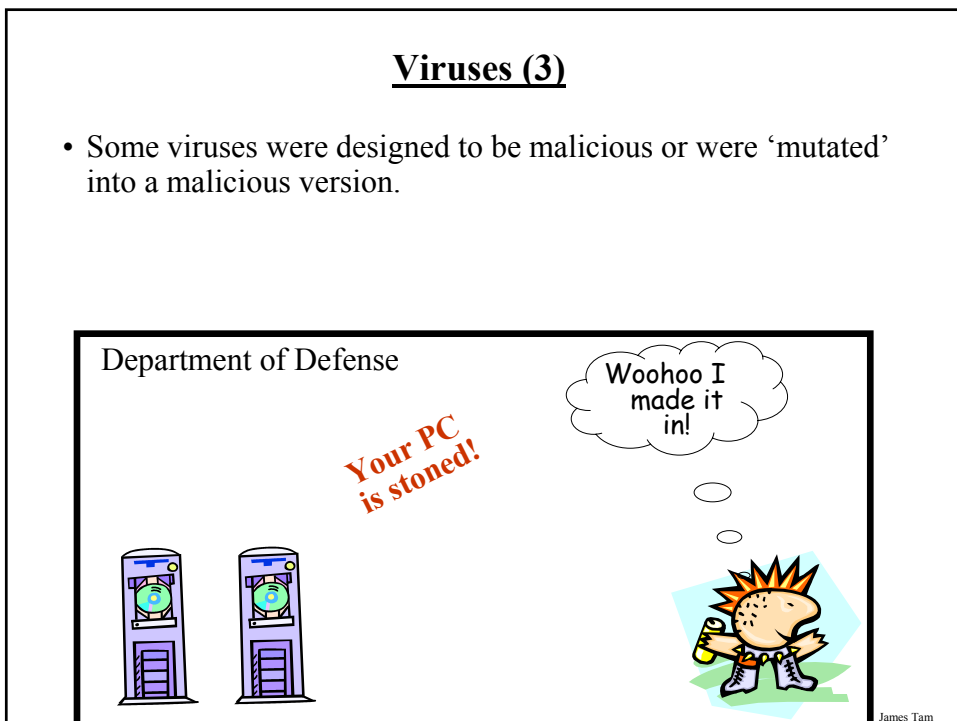
Viruses (2)

- For early virus writers the goal was simply infiltration of a computer or network.
- At most the virus would result in some minor mischief



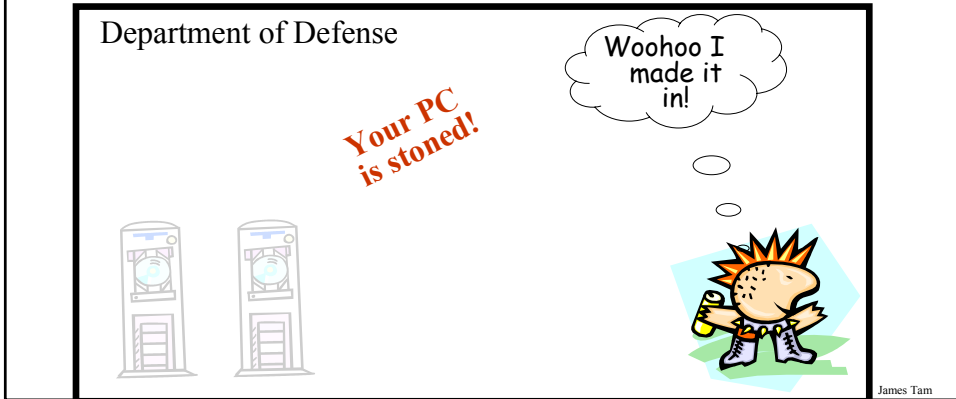
Viruses (3)

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



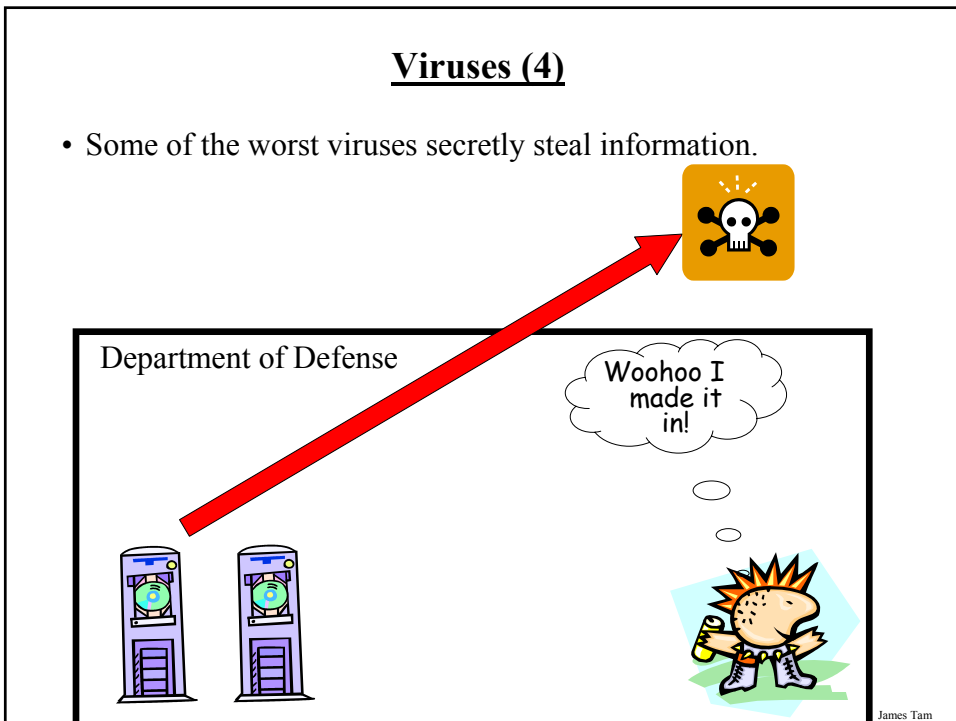
Viruses (3)

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



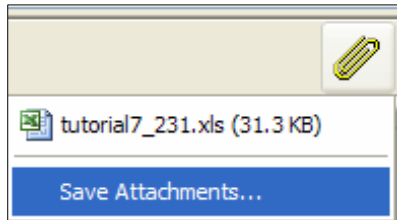
Viruses (4)

- Some of the worst viruses secretly steal information.



Viruses (5)

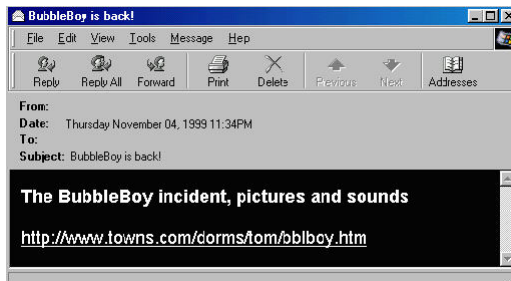
- Require human-intervention to spread.



James Tam

Worms

- Unlike a virus a Worm can spread without human intervention.



James Tam

Macro Viruses

- Macros can be added to many documents.
- 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.

James Tam

Trojans / Trojan Horse

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



James Tam

Protection Against These Forms Of Malware

- Malware discussed so far
 - Viruses
 - Worms
 - Macro Viruses
 - Trojans / Trojan Horses
- Use an anti-virus program:
 - Something is better than nothing (some are free!)
 - 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).

James Tam

Spyware



- 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.

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

(From Internet Privacy for Dummies)

“You hereby grant [company Y – 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.”

James Tam

Spyware (2)



- However some forms of spyware record and transmit *highly* confidential information.

James Tam

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 with protecting against spyware.

James Tam

Keystroke Loggers

- 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.

James Tam

Preventing/Mitigating The Effect Of Keystroke Loggers

- Install an anti-spyware program.
- Get a firewall.
- Minimize the typing of sensitive information with automatic form fillers:

Sign On

WARNING: Protect your confidential information!

I agree to SIGN OFF* when I am finished my Web Applications and Portal sessions:

1. **Sign off*** all Web Applications (such as PeopleSoft, Blackboard, Webmail).
2. **Sign off*** from my Portal (My UofC) session.
3. Close all active browser windows before leaving my computer.

* Sign off does **not** mean just closing the open window -- **I must click on the Sign Off link.**

eID:

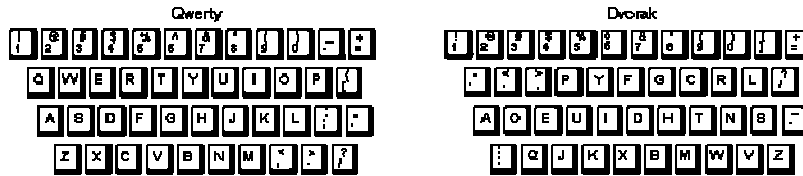
Password:

- Use one-time passwords.

James Tam

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.

James Tam

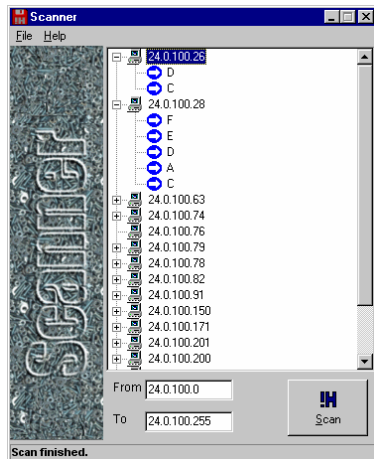
Preventing/Mitigating The Effect Of Keystroke Loggers (3)

- Using low tech methods can also be fairly effective for many keystroke loggers by ‘scrambling’ the text entered or by minimizing (or avoiding altogether) the amount of text entered.

James Tam

Always-On Connections Provides An Easier Target

- Some malicious programs constantly scan computers on the Internet for vulnerabilities (insecure connections):



James Tam

Evaluating The Effectiveness Of Your Firewall

- Firewalls may help to secure your computer by blocking insecure connections.
- 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 e.g., <http://www.grc.com/freepopular.htm>

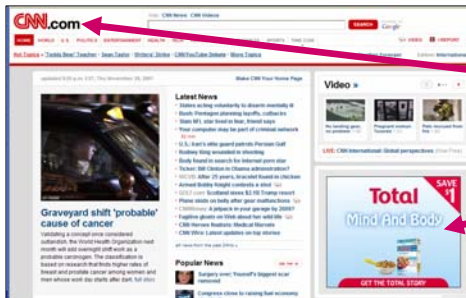
James Tam

Browser Cookies

- Used to store information relevant to the pages that you visit.

```
utma  
14983462.187187  
ama.ab.ca/  
1600  
2350186496  
32111674  
3155248816
```

- First vs. third party cookies



May have 1st party cookies

May have 3rd party cookies

James Tam

Browser Cookies

- Session cookies
 - Disappear after a fixed amount of time or after a session has ended
- Caution: disabling all cookies may not allow many pages to be viewed properly

James Tam

General Ways Of Increasing The Security Of Your Computer

- 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.
- Avoid leaving your computer on all the time (you present a fixed target).
- 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.
- If your computer appears to be acting abnormal then you may try scanning for suspicious processes.

James Tam

You Should Now Know

- What are some common web-based security issues
- What is malware
 - What are some common categories of malware
 - How do the different forms of malware get onto your computer
 - How do they threaten your computer
 - How to protect against each of them
- How does an 'always on' Internet connection effect the security of your computer, how can these threats be reduced
- What is a browser cookie
- What are the different types of cookies and how do they differ
- General ways of increasing the security of your computer

James Tam