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

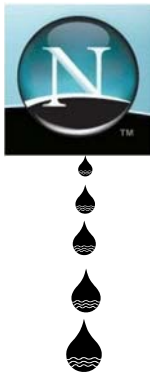
This guy!!!

James Tam

Browsers Are Leaky

Computer IP, geographic location

Computer IP, geographic location



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

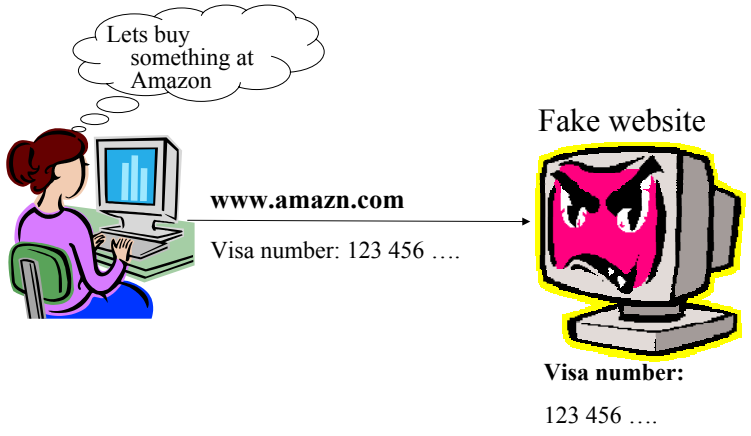
James Tam

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



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

Storing Financial Information

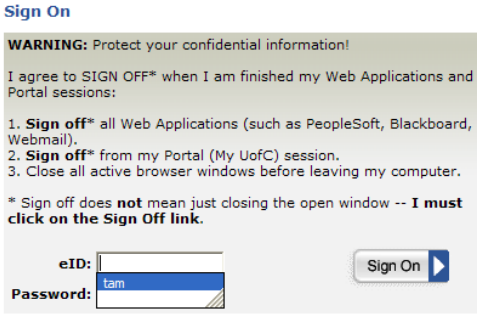
- Even if you enter your information at the correct web site the convenience must be balanced out vs. security concerns:

Storing Financial Information (2)

- Balance the convenience of having this information stored with the merchant (so you don't have fill it) vs. the cost of having it stolen.
- Consider:
  - The size of the merchant (large with the option to spend lots of 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 rather than just vague guarantees).

Saving Previously Entered Information

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

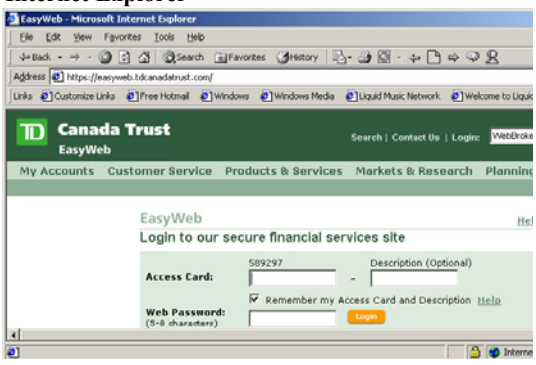


Transmitting Information On The Internet

- Many protocols transmit packets in an unencrypted format.
  - Email
  - Http

- Indicators that a web page employs encryption

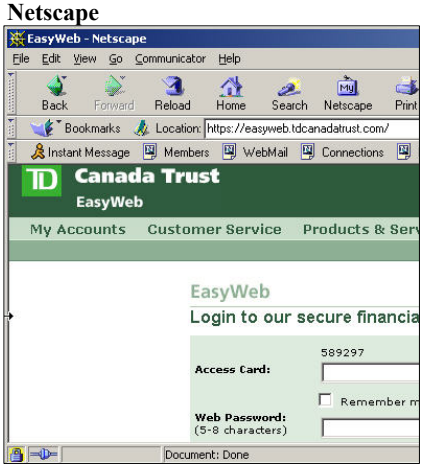
Internet Explorer



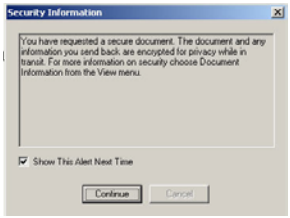
Transmitting Information On The Internet (2)

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

Netscape



General

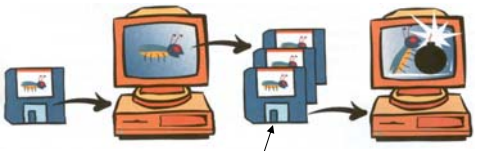


Malware ("Malicious Software")

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

Viruses

- Similar to a biological virus

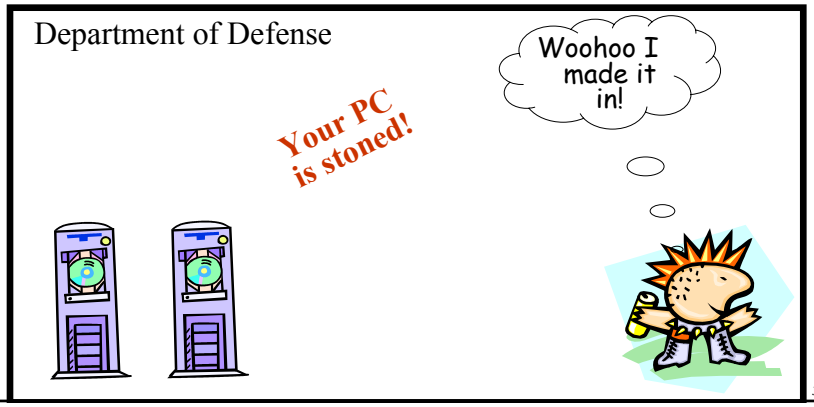


The infection and the replication process may produce symptoms

James Tam

Viruses (2)

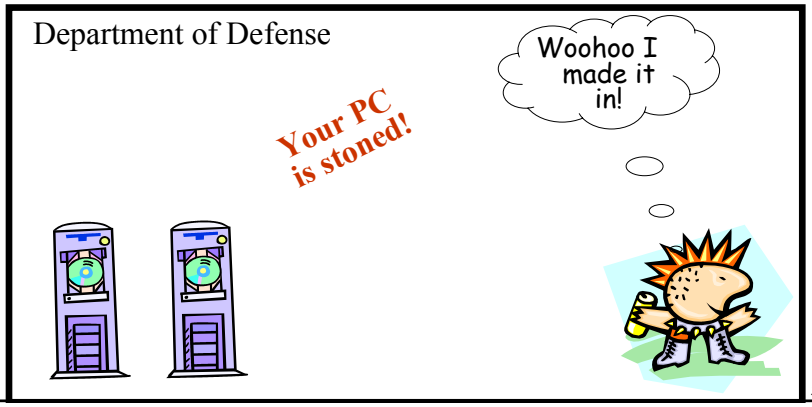
- For early virus writers the goal was simply infiltration of a computer or network.
- At most the virus would result in some minor mischief



James Tam

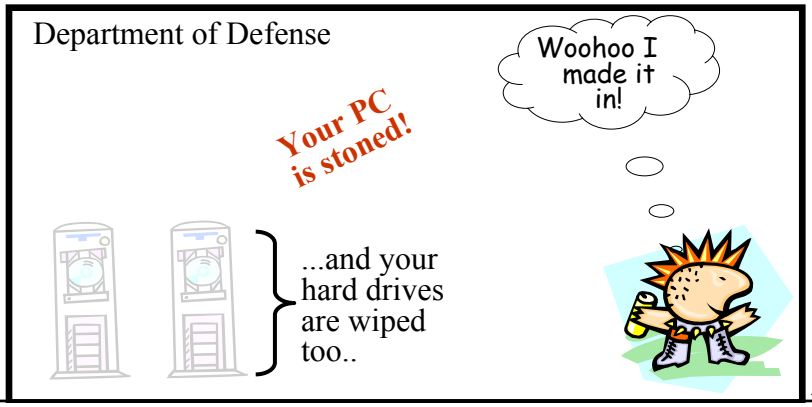
Viruses (3)

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



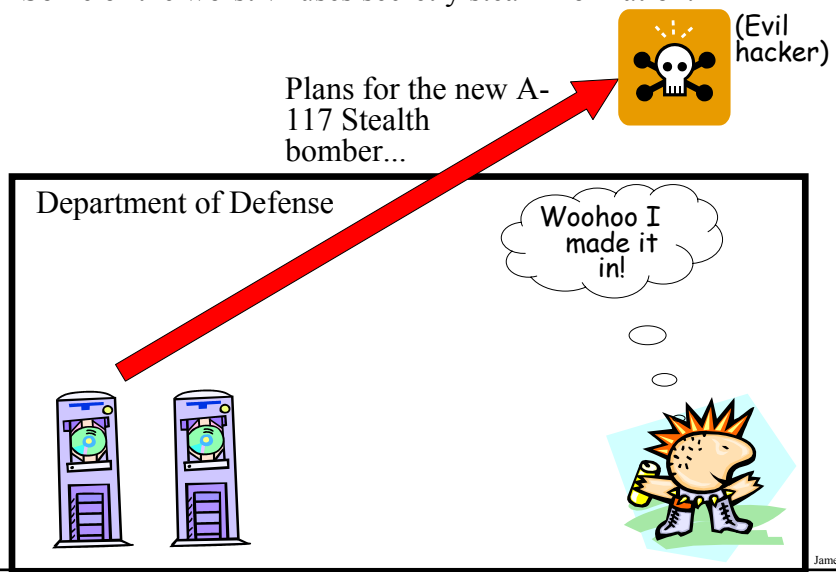
Viruses (3)

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



Viruses (4)

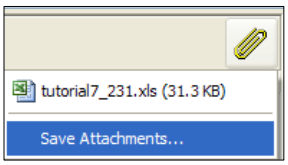
- Some of the worst viruses secretly steal information.



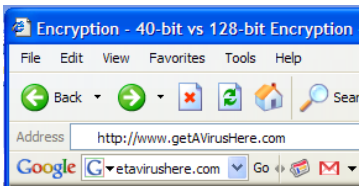
James Tam

Viruses (5)

- Require human-intervention to spread.
  - Email attachments



  - Web-based

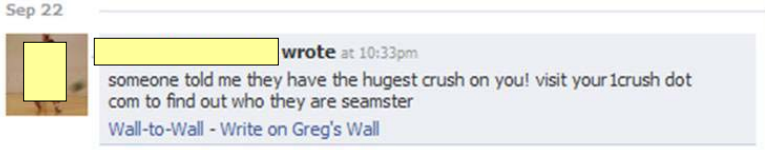


James Tam

Viruses (6)

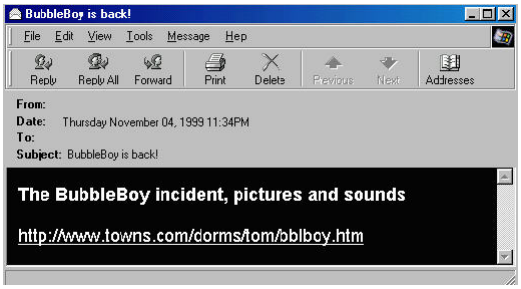
- Trusted websites may unfortunately be used as part of a virus attack.
- Example:
  - Facebook Virus Infecting 'Friends' List: Prompts Users to Download Video
    - http://www.canada.com/globaltv/ontario/story.html?id=48291ac4-f3c5-465c-b172-80299e4ca5dc
  - Provocative messages from your contacts that tempts viewers to follow a link:

Legitimate message from a friend or a virus?



Worms

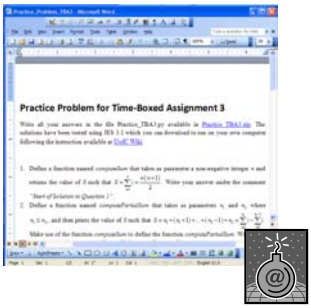
- Unlike a virus a Worm can spread without human intervention.



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.

Original document: infected



Documents made with that application contain the infection

James Tam

Trojans / Trojan Horse

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

The Internet

Some new application that allows you save videos from Youtube$_{TM}$!

Get a cheap hacked version of some commercial software.

Download a special viewer to see "astonishing" pictures/videos of your favorite celebrity.

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!)
    - 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
    - (Also recall that U of C students and staff get free access to – an older – version of McAfee: http://www.ucalgary.ca/it/security/antivirus)

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."

Spyware (2)

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

Protecting Against Spyware

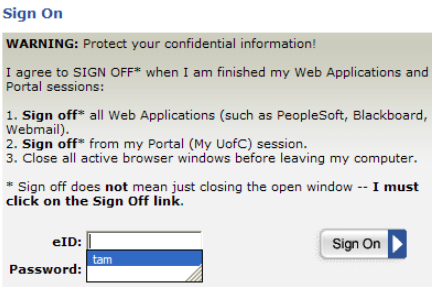
- Some anti-virus programs have begun to expand their services to protect against spyware.
- However there are programs that are dedicated solely with protecting against spyware.
  - Ad Aware: www.lavasoft.com
  - Spy Sweeper: www.webroot.com
  - Spybot: www.spybot.com

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

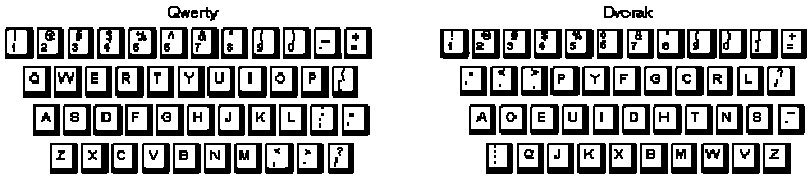
- Install an anti-spyware program.
- Get a firewall.
- Minimize the typing of sensitive information with automatic form fillers:



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

Preventing/Mitigating The Effect Of Keystroke Loggers (2)

- Use an alternative keyboard layout:



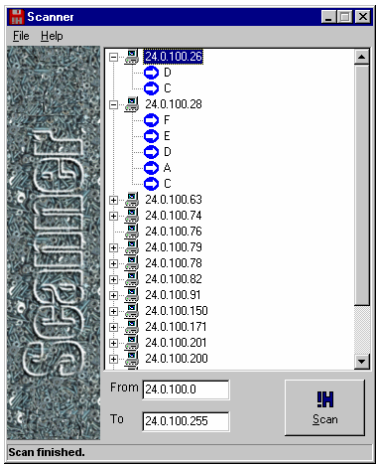
- Fully custom keyboard layouts can be created using tools like the Microsoft Keyboard Layout Creator.

Preventing/Mitigating The Effect Of Keystroke Loggers (3)

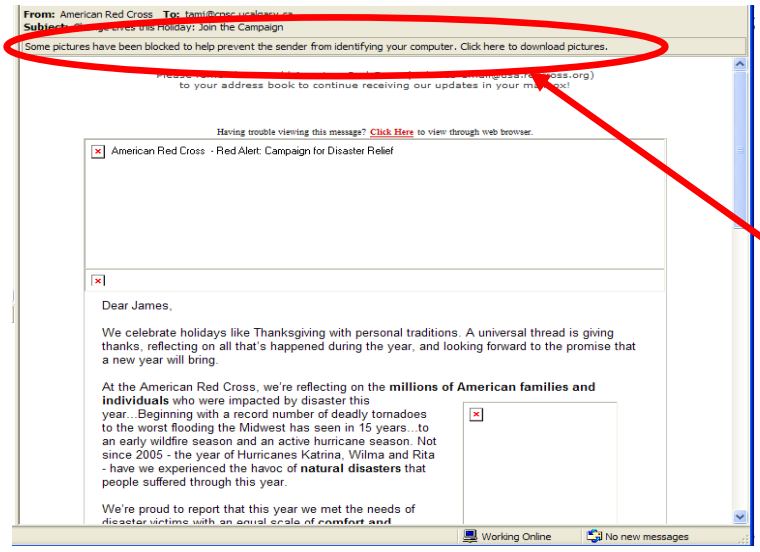
- Using low tech methods can also be fairly effective for many keystroke loggers by ‘scrambling’ the text entered or by minimizing (or avoiding altogether) the amount of text entered.

Always-On Connections Provides An Easier Target

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



Letting Your IP Address Out Can Make You A Target



Often blocked for good reason

JT's note: this particular email is probably safe.

Evaluating The Effectiveness Of Your Firewall

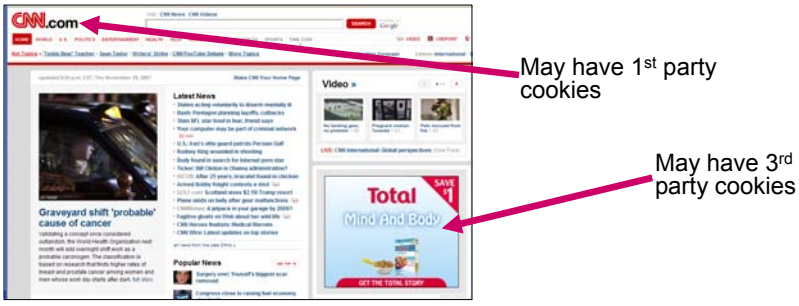
- Firewalls may help to secure your computer by blocking insecure connections.
- If you are unsure of how to configure your firewall:
  - Use the default or recommended configuration
  - Use a trusted source to evaluate the security of your firewall e.g., http://www.grc.com/freepopular.htm

Browser Cookies

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

```
__utma
14983462.187187
ama.ab.ca/
1600
2350186496
32111674
```

- First vs. third party cookies



Brower 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

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.
- Use utilities like the Task Manager to see what processes are running and if unfamiliar ones are taking up most of your processor time.

Scareware

- In-and-of itself it's 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

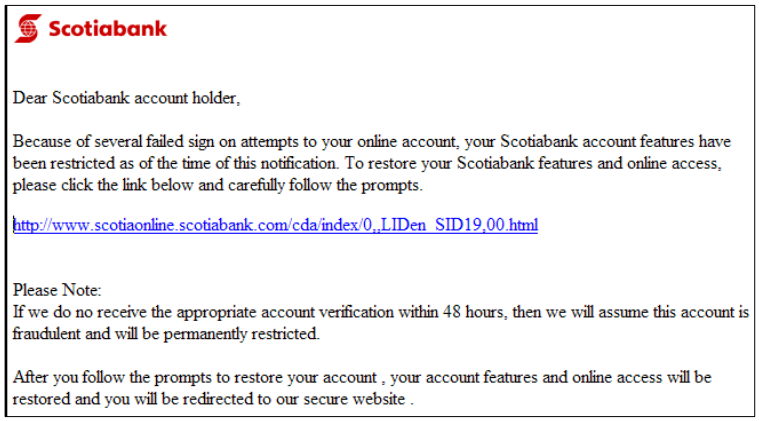
Scareware (2)

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 result in additional problems:
  - Malware infection
  - Credit card theft

Phishing

- Typically it's defined as fraudulent attempts to obtain private information.
- Original attempts at phishing appear quite primitive by today's standards.



Scotiabank

Dear Scotiabank account holder,

Because of several failed sign on attempts to your online account, your Scotiabank account features have been restricted as of the time of this notification. To restore your Scotiabank features and online access, please click the link below and carefully follow the prompts.

http://www.scotiaonline.scotiabank.com/cda/index/0,,LIDen_SID19,00.html

Please Note:
If we do no receive the appropriate account verification within 48 hours, then we will assume this account is fraudulent and will be permanently restricted.

After you follow the prompts to restore your account , your account features and online access will be restored and you will be redirected to our secure website .

Phishing (2)

- Today's phishing scams are more insidious:
  - Virus laden web site
  - Worms that activate with an email

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 employ 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 generally 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.

Posting Information

- While providing and sharing personal details is one of the main benefits of social networking sites such as Facebook, MySpace etc. this must balanced out vs. the potential costs of providing too much information.
  - Providing too information 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.

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.

- One other approach is to provide varying levels of access to your personal information and online activities:
  - Your "real" friends have as much personal information about you online that they have in the real world (don't forget though that the web site operator also has access to this information – read their terms of use because they may be allowed to provide this information to other companies)
  - Your "online/virtual" friends have restricted access to your online information.
  - But keep in mind that your friends may also be subject to identity theft. (Did you your real-world friend actually set up and is currently using their account or does someone else have access to it).

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

You should now know (2)

- Knowing what is scareware, when is/how it is a security threat
- What is phishing and how does it occur
- The importance of keeping aware of and protecting your online privacy
- What is the potential cost of having your personal information online
- How to minimize the risks of providing information online