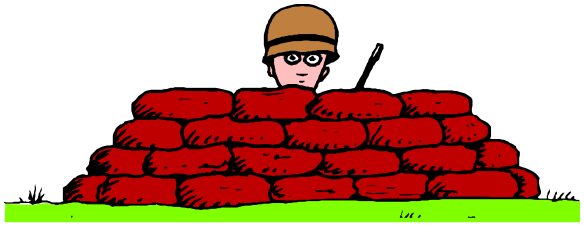
APSGroup

your privacy and security management partner

Security 101

Internet Security & Privacy for Beginners



Disclaimer and Copyright Notice

Copyright on this material is held by Susan Johnson and Geraldine Sombke, but permission is granted for anyone to use this material for security presentations to any public group, so long as any charge for attendance is limited to the direct costs.

Permission is granted to use this material to build upon or develop further materials, provided the original authors receive credit, and the copyright provisions on the developed materials are essentially and substantially the same.

We do not warrant or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information in this presentation. You are reminded to do your own research.

Contents

1. Threats

- Viruses and malware
- Destructive attacks
- E-mail scams
- Identity theft
- Privacy violation / surveillance
- Theft of intellectual property

3. Advanced Topics

- Safe shopping online
- Encryption
- Home networks
- Wireless networks

2. Safeguards

- ✓ Anti-virus programs
- ✓ Keep your system patched
- ✓ E-mail precautions
- ✓ Software firewall programs
- ✓ Backups
- ✓ Passwords
- ✓ Downloading and installing programs
- ✓ Hardware firewalls
- ✓ Safe surfing
- ✓ Protection from Identity Theft

Threats

- Viruses and other malicious software (malware)
- Destructive attacks
- E-mail scams
- Identity theft
- Privacy violation / surveillance
- Theft of intellectual property

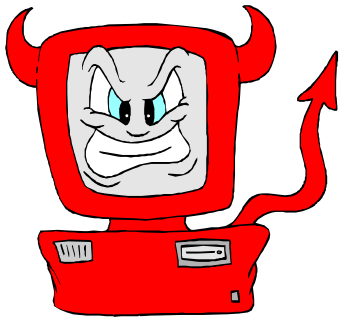
The bad guys aren't new, but the tools are!

Viruses and other malicious software (malware)

- Dumaru
- Naith (Avril, Lirva)
- Sobig
- Bugbear
- Klez
- Braid
- Winevar
- Nimda
- Sircam
- Magistr
- And thousands of others!

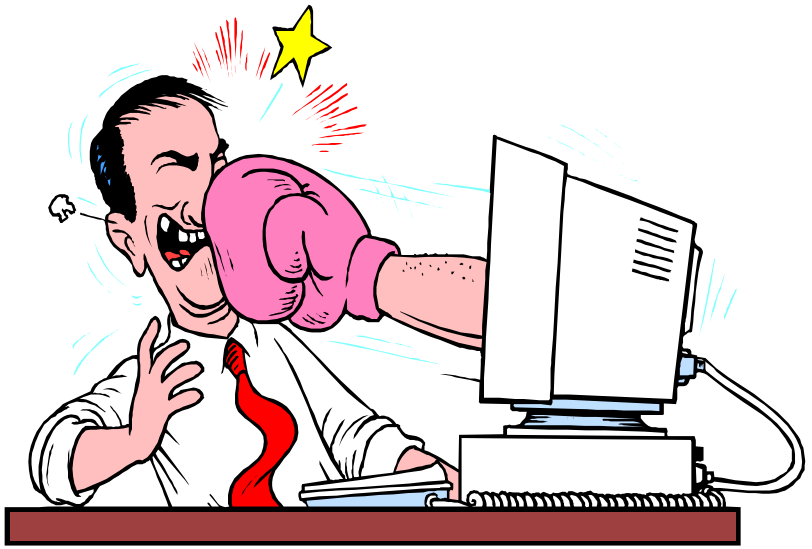
What can malware do?

- Disable security and anti-virus software if it is not detected on entry
- Allow an intruder 'backdoor' access to your system
- Steal your passwords, your personal data, your credit card numbers, your identity
- Delete files from your computer
- Send your personal files or pieces of them randomly to people in your address book
- Use your computer to send spam, store illegally copied music files or host porn sites without your knowledge
- Use your computer to participate in a 'Denial of Service' attack



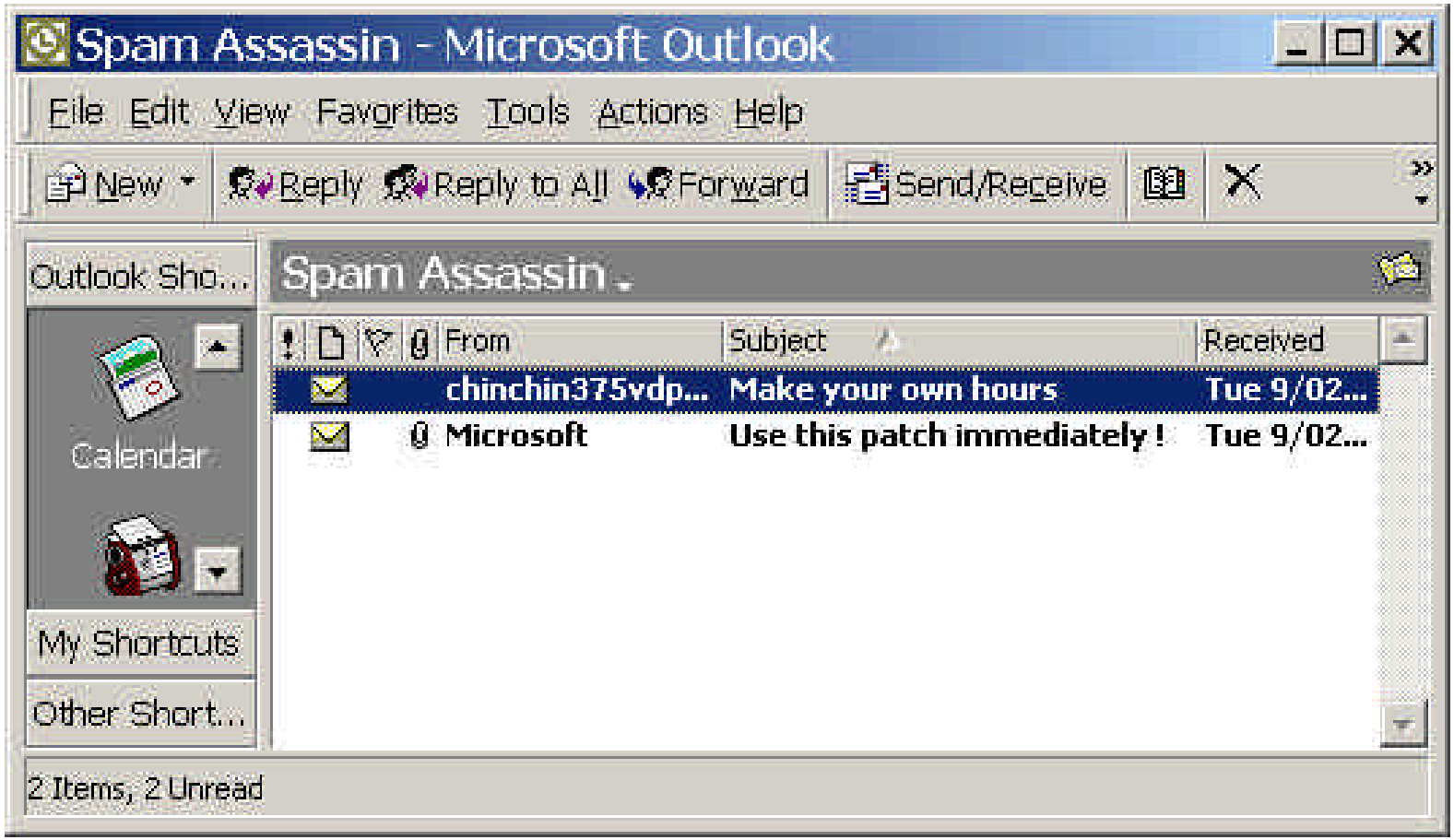
How can you get malware?

- E-mail attachments
- File downloads
- Websites
- Floppies
- CD-ROMs



Check all of these for viruses before opening / using!

E-mail – how viruses get distributed



What to do with it

- Don’t open it! If your anti-virus is up to date, it should have found the virus attachment and deleted it, but don’t take a chance.
- Right click on the message line and click on Message Options. Under Internet headers, you’ll see this info:

  Return-Path: <admin@duma.gov.ru>

  Delivered-To: me@myaddress.com

  From: "Microsoft" <security@microsoft.com>

  To: < me@myaddress.com >

  Subject: Use this patch immediately !

- Note the Return-Path, NOT the From:, which is obviously spoofed. Microsoft doesn’t send patches via e-mails to its customers!

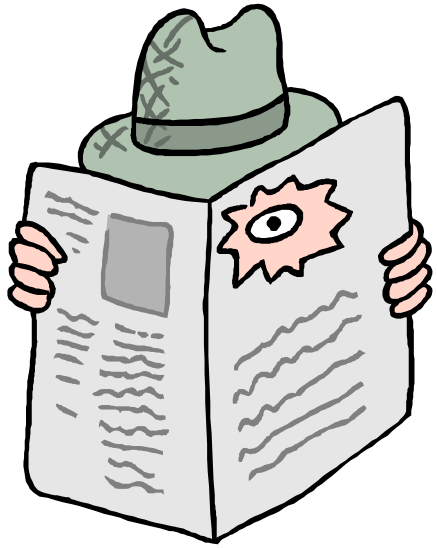
The 'Bad Times' virus

- Deletes anything on disks within 20 feet of your computer.
- Demagnetizes the stripes on ALL of your credit cards.
- Programs your phone auto dial to call only 900 numbers.
- Mixes antifreeze into your fish tank.
- Leaves dirty underwear on the coffee table when you are expecting company.
- Replaces your shampoo with Nair and your Nair with Rogaine
- Leaves the toilet seat up and your hair dryer plugged in dangerously close to a full bathtub.
- Etc. etc.
- **WARN AS MANY PEOPLE AS YOU CAN!!

Note: This is an example of a hoax, whose only purpose is to encourage you to clog up the e-mail system with warnings!

Spyware and trojans

- Comes from companies you thought you could trust: utilities, streaming media players, “free” software
- Reports back to the company on what you watch or listen to
- Circumvents corporate and personal firewalls by setting itself up as a browser “plug-in”
- May be a RAT! (Remote Access Trojan)



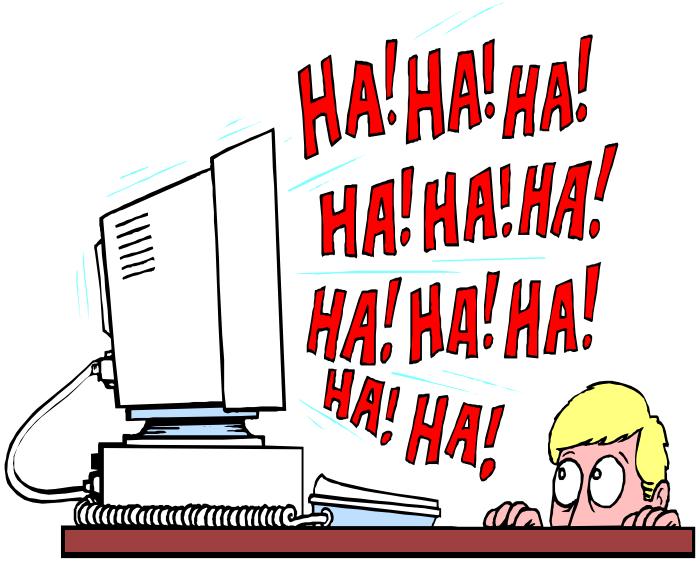
Destructive attacks

- Distributed Denial of Service Attack (DDoS)
- Hackers 'persuade' you to let them infect your computer via e-mail, downloads or direct attack
- The hacker then uses infected computers, especially those with broadband connections, as 'zombies' to flood corporate websites with frivolous requests for access, thus depriving legitimate users of access to the site
- Targets have included Microsoft, the FBI, the White House, Network Associates, New York Times, Yahoo, CNN.com, Amazon, eBay

DDoS -Why should you care?

- Being a good Netizen means that if you can reasonably prevent your computer from being used for illegal or unethical activities, you should do so
- Possible legal liability for the owner of the zombie computer!

E-mail scams



- Nigerian scams
- Various get-rich-quick schemes
- Same con artists as ever, just a new medium and easier to target more dupes
- Remember – if it sounds too good to be true, it probably is!
- Use your e-mail filter to screen most of these out based on key words in the subject or body
- Add senders to your 'Junk Senders' list

Identity theft – How does it work?

USA FTC's Identity Theft Clearinghouse – most typical types of identity theft:

- Credit card fraud
- Bank fraud
- Communications services
- Fraudulent loans

Identity theft – How prevalent?

- "Every 79 seconds, a thief steals someone's identity, opens accounts in the victim's name and goes on a buying spree." CBSnews.com, Jan 25/01
- Consumer groups estimate that as many as 750,000 people a year may be victimized by identity theft.
- It cost the average victim more than $1,000 to cope with the damage from identity theft, according to the FTC.

Identity theft complaints – some Canadian statistics – 2002

PROVINCE	TOTAL	$ LOSS
Ontario	3,831	5,436,655
Quebec	1,480	1,115,698
British Columbia	995	906,286
Alberta	597	590,236
Manitoba	190	165,954
Nova Scotia	177	138,933
Others	359	196,683
TOTALS	**7,629**	**$8,550,445**

Source: PhoneBusters.com

Privacy violation – Cookies

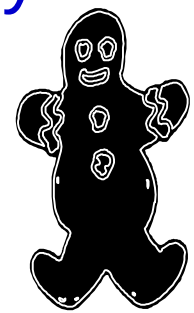
- Definition - "a small text file which is deposited on your hard drive by a web site you visit. This file identifies your computer. It records your preferences and other data about your visit to that site. When you return to the site, the site knows who you are."

  The Privacy Foundation

- Cookies were created for a very good reason – to solve the internet's equivalent of Alzheimer's disease.
- Cookies are required to use many websites and for electronic commerce – e.g. Amazon

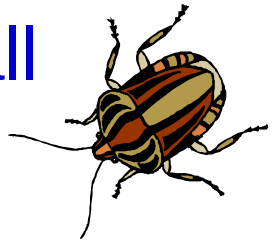
The Darker side of Cookies

- They can contain user names and credit card numbers that have been supplied via forms
- Programming for cookies may have security holes.
- Cookies are used for the "targeting" of advertisements to individual users
- They can also be placed by third parties – i.e. ad networks, not the site you are visiting.
- Cookies can be abused for more sinister reasons than sending 'targeted' ads – e.g. tracking your online research into controversial topics



Privacy violation – Web Bugs

- Definition - "a graphic on a Web page or in an Email message that is designed to monitor who is reading the Web page or Email message."
- They are called 'bugs' to denote a small eavesdropping device, rather than a programming error.



- Used to 'personalize' banner ads based on your browsing history
- In junk Email messages, used to synchronize a Web browser cookie to a particular Email address so the website will know the e-mail address of people who come to the site later.

Privacy Violations by Employers and Governments

- Employers – 14 million employees have their e-mail monitored in the USA
- Government surveillance
  - USA – Carnivore e-mail surveillance
  - Canada – CCRA airline passenger database

- "In a world where most communications are unencrypted, encrypted communications are probably routinely recorded. The mere indication that the conversers do not want to be overheard would be enough to raise an alarm."

  Bruce Schneier, Secrets and Lies

- Think those files you deleted from your hard drive are really gone? Guess again!

Theft of intellectual property

- Music and entertainment piracy is widespread - Napster, Kazaa etc.
- Problem is not new, but the digital format lends itself to copying and widespread distribution
- What if you had written a book and others could read it without paying?
- Copyright limitations include fair use (as in private copying and criticism)

Software Piracy

- The Empire strikes back! Win XP and 'activation'
- There are alternatives:
  - Cheaper versions – e.g. Works or Wordpad vs. MS Word
  - Linux and Star Office
  - Freeware and shareware products for Windows
  - As a bonus, you may be less susceptible to viruses which are targeted at ubiquitous Microsoft products

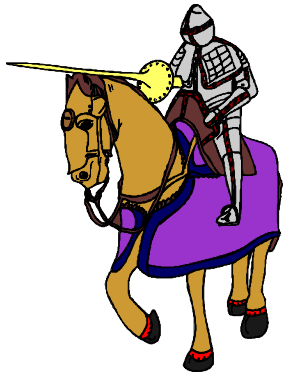
Peer-to-peer (P2P) file sharing networks - the risks

- P2P software may contain trojans
  - Fake mirror site for downloading
  - Advertiser applications (see Altnet)
- P2P files (e.g. MP3) are a popular way to distribute malware
- Disclosing one's 'real' IP address
  - Filetopia encrypts the data session
  - But what if the other user is the bad guy?

Peer-to-peer (P2P) file sharing networks - the risks (cont.)

- File sharing
  - Intended - your computer used to store pirated copies of music files
  - Unintended – all files on your computer may be accessible if the software is not properly configured
- Resource sharing
  - For good causes – SETI, mapping genomes, AIDS research - Entropia
  - For 'not-so-good' causes – your computer used to serve Internet ads or host porn sites!

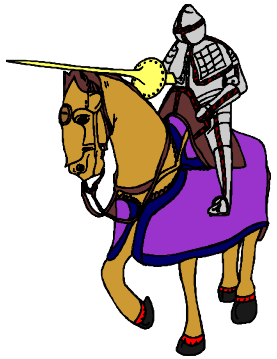
Safeguards



Now that we've really scared you, and before you go home to sell your computer and cancel your Internet access, let's talk about what safeguards you can use to protect yourself from these threats!

Safeguards

1. Install and use anti-virus programs
2. Keep your system patched
3. Use care when reading e-mail with attachments
4. Install and use a software firewall program
5. Make backups of important files and folders
6. Use strong passwords
7. Use care when downloading and installing programs
8. Install and use a hardware firewall
9. Practice safe surfing
10. Protect yourself from Identity Theft



Sources: CERT Coordination Center, AND the Privacy Commissioner of Canada

1. Install and use anti-virus programs

- "If your financial resources are limited, they are better spent purchasing a commercial anti-virus program than anything else." CERT
- Most anti-virus programs use 'signatures' or profiles to identify potential viruses
- Keep the signatures updated, preferably daily or via automatic updates from the vendor
- Set the a/v program to run in the background, scanning e-mail messages as they arrive
- Scan any new files before opening them
- Run a scan on your entire system – preferably daily (overnight), and at least weekly

If you think you already have a virus

- Ensure you have up-to-date anti-virus software and definitions installed
- Review the analysis and disinfection instructions on your anti-virus vendor's web pages – you may have to install in MS-DOS mode
- Disconnect the computer from the Internet and your home network
- Scan your entire system for viruses
- Go to the anti-virus vendor's web site to find out what they suggest, if the software doesn't automatically remove it.

2. Keep your system patched

- Patches are often issued to fix security vulnerabilities
- Sign up to a mailing list for update notices from the vendor
- Use automatic updates if you trust the vendor, or set them to just notify you
- Check whether the patch can be 'undone' if it creates problems with other apps

3. Use care when reading e-mail with attachments

- Don't open messages from strangers
- Don't open messages with attachments from friends unless you were expecting the attachment
- Don't rely on the subject line or the sender name – both can be spoofed
- Have your anti-virus software check your e-mail as it comes in, but don't rely on it
- Turn off the preview pane!
- Change your Inbox view so it displays the icon for attachments (paper clip)
- Don't hide file extensions

4. Install and use a software firewall program

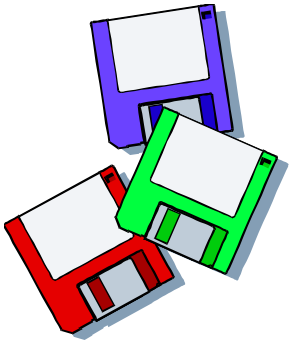
- Like a security guard at an office building who decides who can come and go
- Must have rules to help them decide
- A firewall program looks at every 'packet' destined for or sent by your computer, and determines whether to allow it to continue to its destination based on rules you set
- Popular software firewalls – ZoneAlarm, BlackICE, Norton Internet Security

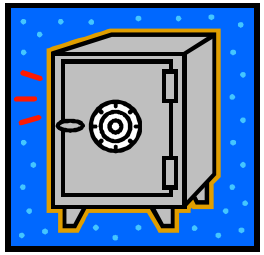
Configuring the firewall

- You can set rules to allow only access out, BUT what if a bad guy is already in your system? This is THE major weakness of XP's basic firewall.
- You should look at each program you use regularly, and determine whether it needs Internet access to function
- Good firewall software should be able to learn your rules, but the first couple of weeks may be a pain
- Make a backup of your rules once they're complete, if the software allows this
- Don't forget to password protect the settings on your firewall software

5. Make backups of important files and folders

- Decide which files to back up – usually data, not programs
- Decide how often they should be backed up
- Decide what media to use – floppies vs. CD-ROMs vs. a second hard drive vs. a drive on another computer on your home network vs. online services
- Decide where to store the backup – preferably in a fireproof container or offsite
- Consider using Drive Image or Norton Ghost to take a snapshot of your system, especially before installing new programs





6. Use strong passwords

- A strong password should not be a dictionary word, unless additional numbers or characters are added randomly into it. Password 'crackers' love dictionaries.
- Don't use the same password for online banking or brokerage that you use for accessing content sites.
- Don't use the same password online as you do on your computer (if you share the computer)
- It's okay to write the passwords down somewhere safe, such as in a sealed envelope off the premises – NOT on the computer monitor!

7. Use care when downloading and installing programs

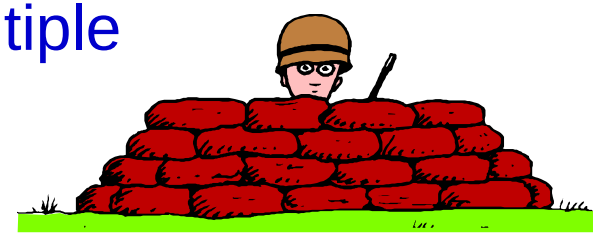
- Remember, programs run with the same privileges as you have
- First, do you really NEED the program?
- Basic precautions:
  - Is it purchased from a reputable commercial site?
  - If not, was it downloaded from a reputable shareware site which virus-checks their programs?
  - Beware of free lunches and ‘free’ software!
  - Scan it with your anti-virus software
  - Take a snapshot of your system first

7. (Cont). Avoiding spyware

- Avoid any software that transmits information about your activities, no matter what promises the vendor makes.
- Install utilities such as PestPatrol, Ad-Aware or Spy Sweeper that can detect spyware – but only download from recognized vendors or shareware sites such as Tucows.com!
- Like anti-virus, keep definitions up to date.

8. Install and use a hardware firewall

- Why a hardware firewall?
  - Hardware firewalls completely hide your IP address from the Internet
  - Better protection than a software firewall
  - Can be used to allow a single Internet connection to be shared by multiple computers



- Good products:
  - Linksys EtherFast Cable/DSL Router allows sharing between up to 4 machines
  - D-Link DSL/Cable Residential Gateway
  - NetGear RT314 Cable DSL Gateway Router
- Prices vary from $49-$189

9. Practice Safe Surfing

- Be careful what information you give out
- Use dummy e-mail accounts
- Keep your browser from blabbing on you
- Opt out wherever possible
- Consider using an anonymizer account, especially for dodgy sites – www.anonymizer.com
- Clear your memory cache after surfing, if others share your computer
- Don’t accept unnecessary cookies and use inexpensive 'Cookie buster' software to block or remove cookies from your hard drive – e.g. Cookie Crusher ($15)
- Download Bugnosis to make web bugs visible - www.PrivacyFoundation.org

10. Protect yourself from identity theft

- Be careful about sharing personal information – ask why it is needed, how it will be used, who will be sharing it, and how it will be safeguarded
- Burn or shred personal financial information such as statements, credit card offers, receipts, insurance forms, etc.
- Don't use obvious passwords – birth dates, mother's maiden name
- Monitor your credit rating and pay attention to your credit card and utility billing cycles

Privacy Commissioner of Canada
http://www.privcom.gc.ca/fs-fi/02_05_d_10_e.asp

Summary

- Remember, for every online threat, some enterprising company or organization or individual has developed a safeguard
- Aim for defense in depth – e.g. hardware + software firewalls
- Use your common sense
- Try to be cautious, not paranoid

Advanced Topics

Safe shopping online

Encryption

Home networks

Wireless networks

Steps to Safe Shopping Online – 1

- Check out the merchant's ratings – ZDNet Shopper, Yahoo Shopping, Epinions
- Read the fine print
  - What is their return policy?
  - Do they offer a refund or store credit?
  - What is the cost of delivery?
  - Contact information?
- Check out the privacy policy and look for Opt Outs.

Steps to Safe Shopping Online - 2

- Look for the closed padlock icon which indicates encryption for ordering. Check the certificate matches the site name.
- If there is no padlock, check the URL and make sure you're still on the right site. Don't proceed with the order.
- Never send payment information through e-mail. E-mail is not encrypted, so it's not protected.
- Don't let them store your credit card details for 'one click ordering'. IF their site is hacked, your card details could be exposed.
- Use a credit card, NOT a debit card. You have no liability with Visa, Mastercard or American Express for any credit card fraud (unless you're the perpetrator!)

Steps to Safe Shopping Online - 3

- Create a paper trail
  - Print off records of your purchases in case you should need them to return or exchange items.
  - Note the merchant's Internet address.
  - Save e-mailed purchase confirmations.

- Know your privacy rights
  - See the Privacy Commissioner of Canada's website
  - Remember USA-based online merchants will not be covered by Canadian legislation

Use encryption to protect sensitive data

- Encryption isn't new – dates back to 3000 B.C.
- Computers made it practical to encrypt data based on complex mathematical formulas
- Phil Zimmerman made it affordable for individuals to use encryption – Pretty Good Privacy – www.pgpi.org/
- Encryption can be used to send private messages and documents by e-mail and to secure files on your hard drive

Home networks

- If your home network isn't connected to the Web, your risk is low
- If it is, and any computer is running any version of Win 98 or earlier (e.g. Win 95), your entire network is insecure
- Upgrade to Win 2000 if you can find it, otherwise to Win XP
- Get a good book – "Home Networking Survival Guide" or "Home Networking for Dummies"
- Unfortunately, we're all System Administrators now!

Wireless networks

- Operate on radio frequencies
- WEP (Wired Equivalent Privacy) encryption is available with most base stations. Two drawbacks:
  - Easily broken using free programs – e.g. AirSnort
  - Significant performance impact
- War driving and war chalking
- WEP 2 is coming, but new standards take time to be implemented into products
- Bottom line – don't assume your information is private on a wireless network.

Useful Links – A Short List

- Virus Encyclopedia - http://www.viruslist.com/eng/viruslist.html
- Safe Shopping Online - http://www.zdnet.com/anchordesk/stories/story/0,10738,2899248,00.html
- Identity Theft FAQ – http://www.identitytheft.org/faq.htm
- How to uninstall Brilliant Digital's Altnet software- http://news.com.com/2100-1023-875274.html
- Privacy Commissioner of Canada – your rights as Canadians - http://www.privcom.gc.ca/index_e.asp
- Privacy Foundation FAQ: http://www.privacyfoundation.org/

If you only buy one book on security, buy this one:

- Bruce Schneier – Secrets and Lies

For more information or to request a presentation to your organization, please contact:

Susan Johnson, C.A., CISSP
www.APS-Group.com