Secure Your Home Network

Vancouver ISSA - Community Outreach Program

Security Awareness Training

Overview of Securing your Home Network

- What do you need to protect?
- What are the threats?
- How do you protect against the threats?

What do you need to protect?

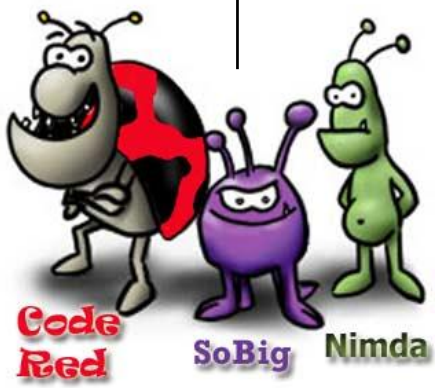
- Information stored on your computer hard disk
  - Privacy of your files: letters, reports, financial statements
  - Accounts and passwords
  - Pictures, Music, Movies
  - Computer settings
- Information stored remotely
  - Email accounts (e.g. Hotmail, Yahoo, Gmail)
  - Bank account information (e.g. RBC, CIBC)
  - Personal web-sites (e.g. www.lookatme.com)
  - School records
  - Health records
- Against losses due to ‘downtime’
- Your personal / private information
- Your safety and the safety of your children

What are the threats?

**Fire,
Accidents, Theft
Spikes, Surges**

**Email
Threats**

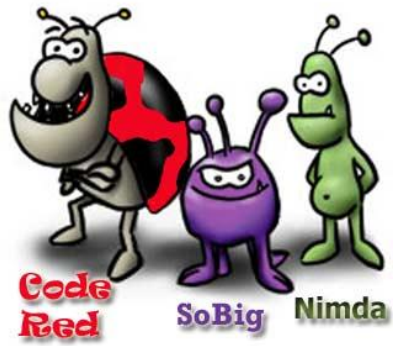
Spyware



Virus, Worms, Trojans

**Hackers /
Criminals**

Malicious Software



- Bugs / Flaws in Programs
- Virus, Worms, Trojans
- How do you contract them?
  - Opening infected email attachments
  - Downloaded and installing programs from untrusted sources (e.g. Internet)
  - Receiving infected files from Instant Messaging applications
  - Visiting web-sites with active content
  - Having an Operating System with out of date patches (worms)

Spyware

- Used to track your activity
- Symptoms
- How do you contract it?
  - Surfing websites (Active X, Java)
  - “Free Sites” – movies, music, porn
  - P2P file share programs (Napster, Kazaa, Limewire)

Hackers

What do they want?

- Challenge / thrill
- Financial profit
- Recruit your computer for their “zombie army’

How do they do it?

1. Scan the Internet
2. Look for computers that are responding
3. Look for weaknesses on computers that respond

Email threats

- Spam
- Phishing (fake e-mail)
- Attachments
- Email hoaxes

Other

- Fire
- Accidents
- Theft
- Hardware failures
- Software faults

- Being used to attack other systems

Why should you be concerned?

Computer Crash / Problems

Violates your Privacy

Identity Theft

Worse…

Computer Crash

- Computer “freezes”, reboots or crashes.
- May lose data or not be able to get up and running again.

Causes:

- Virus or other malicious software
- Hacker
- Faulty hardware (hard-disk, motherboard)
- Software failure (operating system)

Violates your privacy

- View or modify your files
- Record your keystrokes

- Email privacy
- Google privacy
- At the workplace

Identity Theft

- Someone uses your personal information such as your name, Social Security number, credit card number or other identifying information, without your permission

- They then commit fraud or other crimes using your identity

…worse

- Online stalking / harassment
- Children

Same Old Attacks…

- Like the physical world… People populate cyberspace. People interact with each other. They form communities. It is filled with commerce.

- The attacks / crimes are not new, they mirror the physical world:
  - Embezzlement
  - Physical and digital banks get robbed
  - Invasion of privacy
  - Theft, racketeering, vandalism, voyeurism, exploitation, extortion, fraud
  - Cyber stalking
  - Child Porn
  - Money Laundering
  - Cults

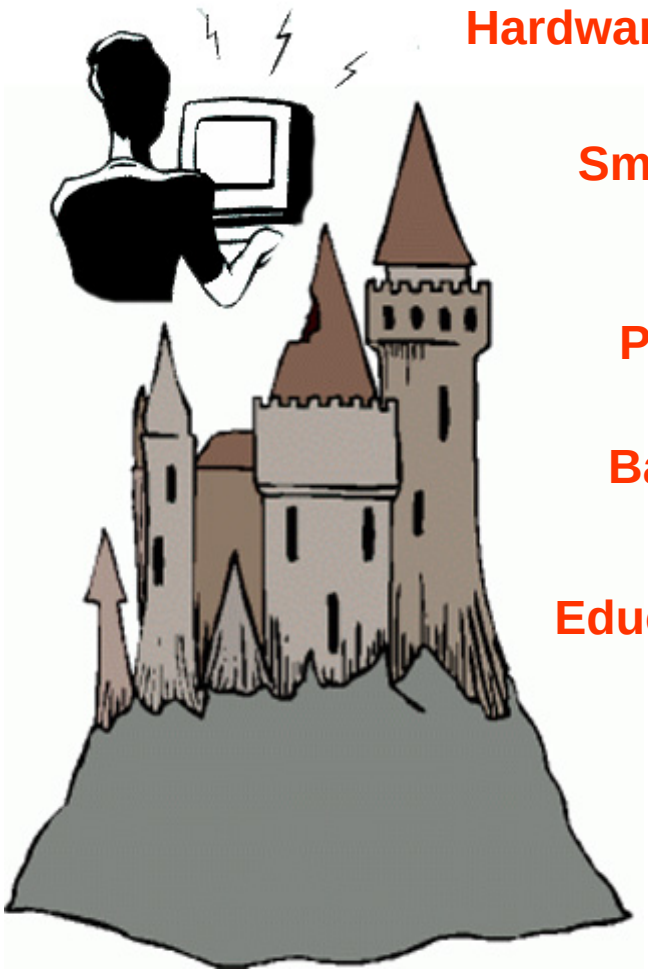
The New Face of Attacks…

- Attacks may have the same motivation and goals, however they can be much more devastating for three main reasons:

  1. *Automation*
  2. *Anonymity*
  3. *Technique Propagation*

- Reactive responses won’t work as they traditionally have.

How do you protect against the threats?



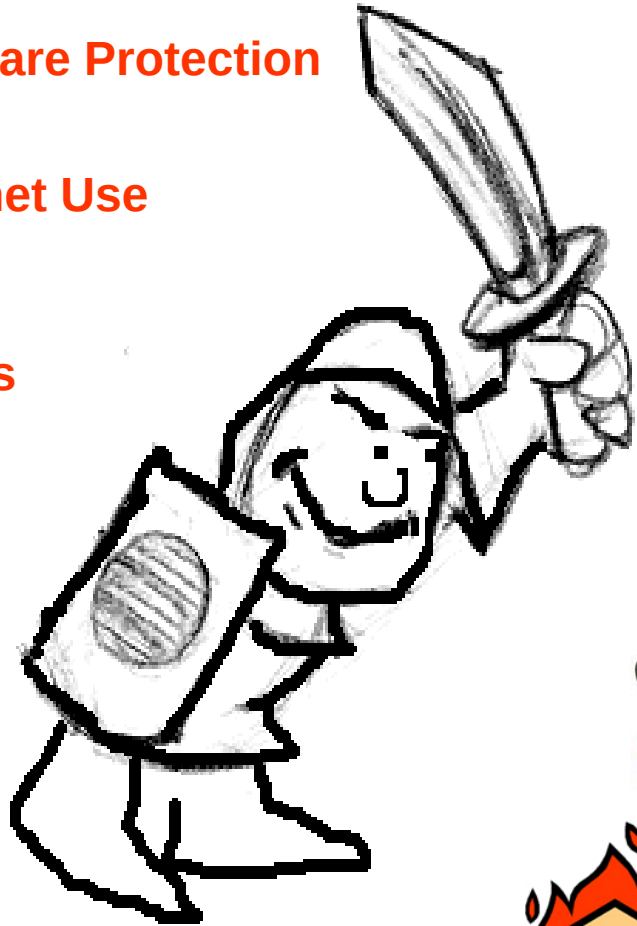
Hardware / Software Protection

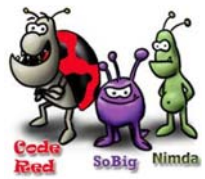
Smart Internet Use

Good Passwords

Backups

Education

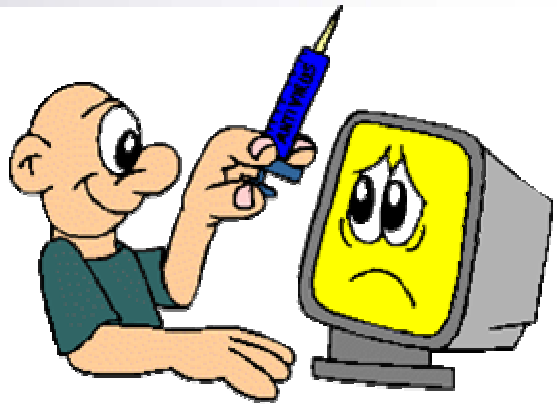




Firewall

- The “front door” to your computer network.
- Use the firewall built-in to Windows XP Service Pack 2, or for greater functionality you may want to consider using another software firewall
- Best solution: use a router between your home computers and the outside world
- You can use the Shields Up! website to see if your firewall is protecting you

Anti-Virus



- Install antivirus software:
  - Best to install this as the first program after a fresh OS install.
  - Configure AV software – auto-updates
- Avoid programs from unknown sources
- Disable Macros in MS Office
- Don’t double click attachments in emails unless you trust the sender / file extension

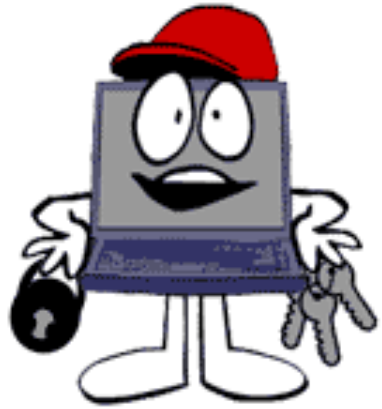
Anti-Spyware

- Install an anti-spyware program
- Don’t blindly install anti-spyware programs offered on the Internet
- Browse slower, read the pop ups!
- Click the ‘x’ or Alt-F4

Updates and Patches

- Microsoft Product Updates:
  - http://windowsupdate.microsoft.com/
- Microsoft Baseline Security Analyzer:
  - www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/Tools/mbsahome.asp
- Macintosh security information:
  - http://www.apple.com/support/security/security_updates.html

Passwords



- At least eight characters
- Random mix of letters, numbers, and special characters
- Develop a passphrase (i.e., 2g00d2BT)
- Change periodically (recommend three month intervals)
- Two / Three levels of passwords

Safe Email Practices

- Attachments
  - Don’t open unknown email attachments
- Spam
- Phishing
- Hoax emails
- Use a “side / anonymous” email account

Safe Web-Browsing Practices

- Filter your browser (limit Active X, Java, Flash)
- Type in Web-Address (URL) carefully
  - E.g. www.google.com not www.googel.com
- Encryption (https://)

Other

- Turn off your computer when not in use
- Disable hidden filename extensions
- Don’t do your banking, etc on computers other than your secured home PC. (e.g. not in a public place, school, etc)
  - Keystroke loggers
- Encrypt sensitive data
- Shred sensitive documents & receipts
- Check bank activities often

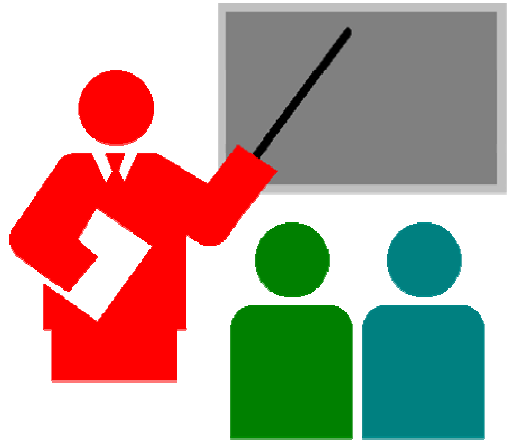
Backups

- Back up your important files
- Options available:
  - CD-ROM burners
  - USB Keys
  - External Hard-disks (USB)
  - Disk image copies
  - Tape Backup
- Keep your backups in a safe place!

Wireless Security

- Default setup is insecure!
- Password Protect Router’s config page
- Disable SSID broadcast
- MAC Address Filtering
- Enable WPA or WEP encryption

Educate your family



- Inform your family and anyone else using your network about good security practices.
- Inform children about Internet threats, including online predators.
- Place computers in a common area where childrens' actions can be monitored

Useful Links

- ISSA Resources Page
  - www.vancouver-issa.org
    - Security links
    - Vendor links
    - Government links
    - Detailed recommendations
    - Latest security information
- Email us!
  - help-me@vancouver-issa.org

Questions?

“Treat the Internet as if was a bad part of town, you need to protect yourself and you can't let your guard down...”

Thank you!

j8 jcrooks001, 10/06/2005