

A decorative graphic consisting of a thin yellow circle on the left side. A thick black bracket is positioned vertically on the left, and a thick yellow bracket is positioned vertically on the right. A horizontal bar with a gradient from olive green to white is centered across the middle, containing the title text.

Protecting Your Identity

How to minimize your potential for ID theft, and what to do if it happens...

DBPI Technology Lab – May 7th 2006

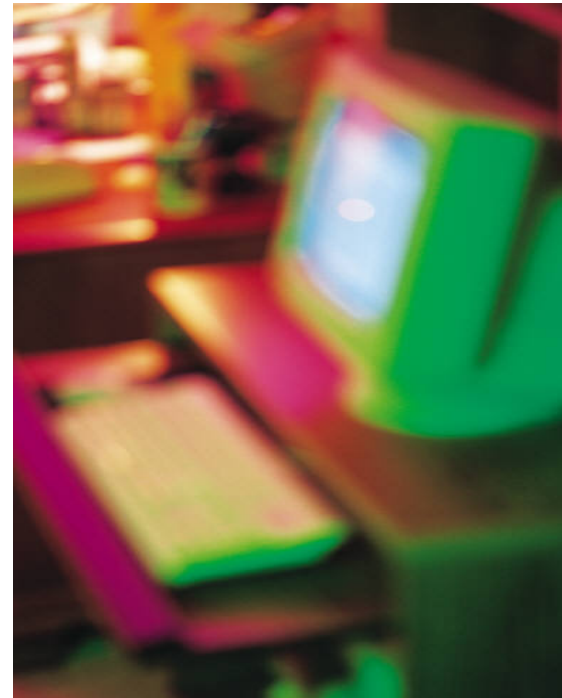
[Introduction]

Who am I?

- Sr. Information Security Consultant
- More than 9 years experience in Information Security
- More than 20 years experience in general IT
- Industry certified...
 - CISA
 - CISSP-ISSAP
 - SSCP
 - NSA-IAM
 - TCP, *etc...*
- **I have been a victim of ID theft myself**

[The Current Situation]

- General weak information security practices *everywhere* – *data breaches happen all the time*
- The Internet is **not** the most common vector, for now...
- Organized crime figured out there's good money in hacking
- Hackers, criminals and even terrorists are actively looking for vulnerable systems to use
- Keyloggers, zombie armies, rootkits, DDoS and spyware...



[A Very Real Threat]



- Point-and-click tools for scanning and hacking systems are freely available on the Internet – **skill is not required**
- There are high quality ID theft cookbooks available on the black market
- Non-importance is a **myth!**
- ID Theft is **FBI/SS #1 crime**
- Federal and State Agencies are still passing the buck
- Sadly, there is no “Silver Bullet”

[A Few Scams]

- **419 (Nigerian)** – extra money for “processing”
- **Lottery** – no, you didn’t really win
- **Account problems** – can you tell us your info?
- **Ransom-ware** – free your data for money
- **LifeFlight** – send us money or else
- **Surgery** – body work on your dime
- **“Evil-Twins”** – fake wireless hot spots
- **Auto ID theft** – yes, ID theft for your car
- **Counterfeit company** – ID theft for your business

If it seems too good to be true... Be skeptical!

[Corporate Data Breaches]

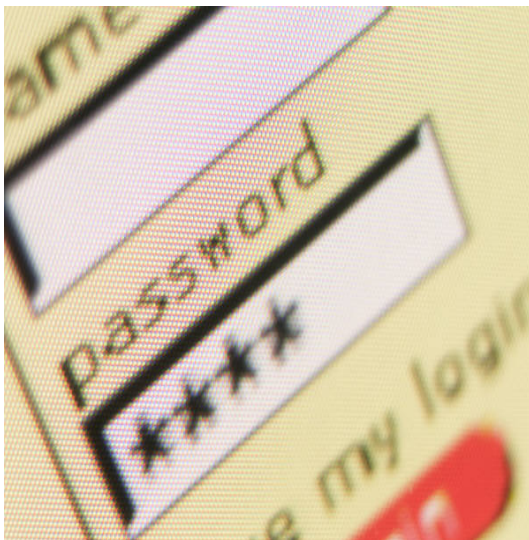
- You don't even have to do anything
- Make sure your information is current
- Actually read the privacy policy
- Opt out when you can
- Support legislation such as SB1386
- Let them know your opinion/position

Why Protect Your ID?

Some impacts associated with ID Theft...

- Loss of funds - possibly *all* funds
- Negative, possibly *severe* impact to credit rating
- Loss of time to clean up credit, bank and Internet accounts
- Loss of time while cleaning/rebuilding affected computers
- Loss of job if your home computer is found to be the source of a security breach at your company
- Loss of reputation; potential negative public image
- Many “intangibles” – many more than you expect
- ***Note: You may receive criminal treatment and investigation for crimes committed using your ID, systems or networks!***

Electronic Information Security

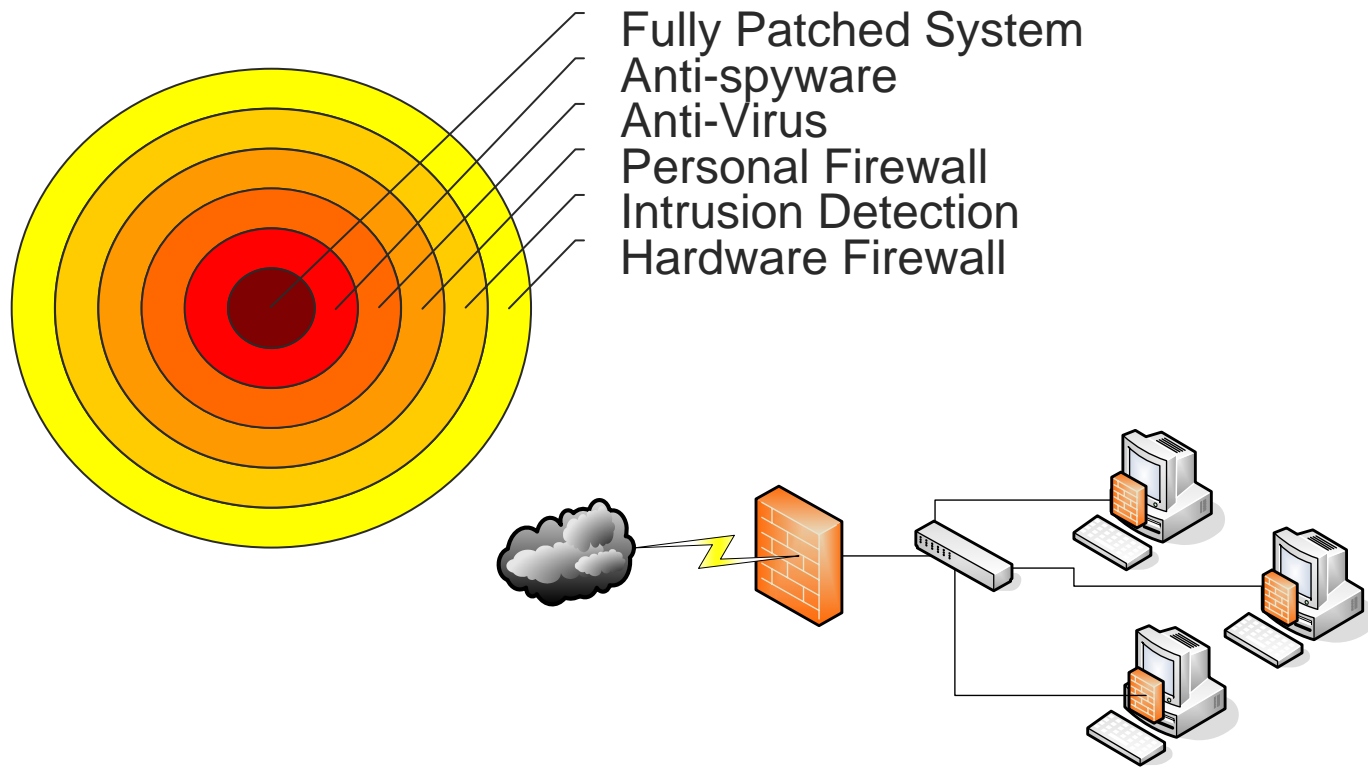


Defense in depth!

It's all about the layers...

- Protection Hardware
- Protection Software
- Patch, *patch*, **patch!**
- **Strong *and* unique passwords**
- Encrypt *when necessary*

[Layered Model]



Some Protection Hardware

- Network Hardware
 - Firewalls
 - Routers/Modems
 - VPN
- USB tokens (thumb/flash drives)
- SecurID
- Biometrics

Note: wireless is dangerous if not used correctly...



[Some Protection Software]



- Personal Firewalls
- Intrusion Detection Systems
- Anti-Virus
- Spyware/Adware Blockers
- Others...
 - Content filters, Pop-up blockers, Cookie crushers, History scrubbers
- All-in-one packages
- Watch out for **snake-oil**
- Encryption...

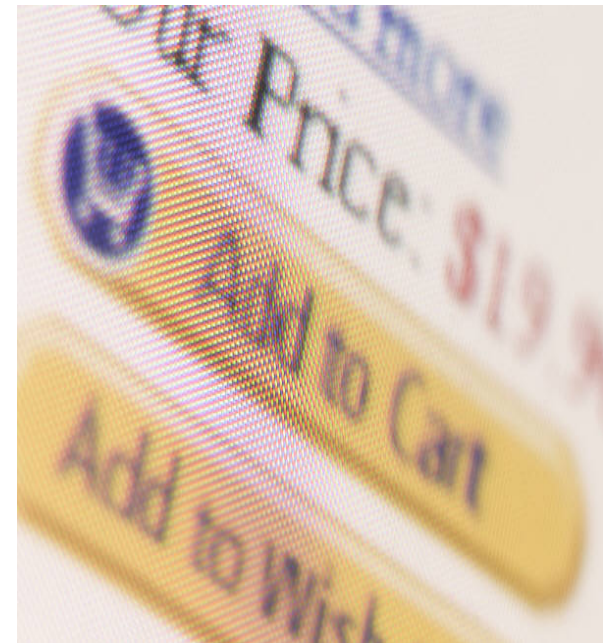
[The Real Encryption Story]

Encryption is good, but...

- **Simple:** use file encryption judiciously
- **Never** lose your keys
- If you do, **don't** count on a locksmith
- Can get very complex, very quickly
- Encryption for data **at rest**
- Encryption for data **in transit**
- *Again, never* lose your keys...

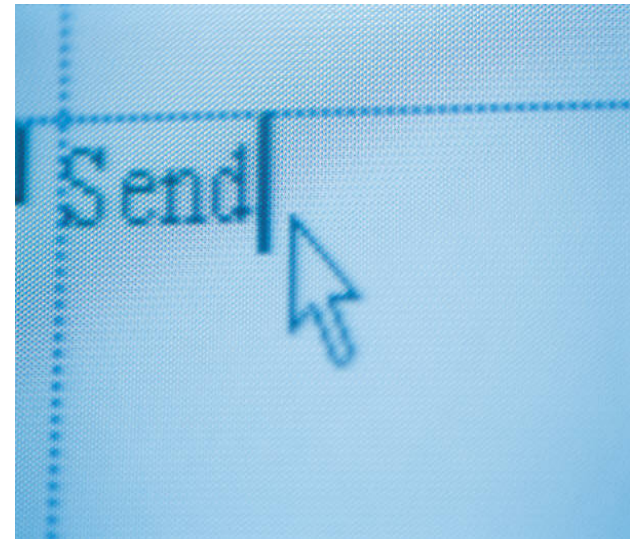
[Internet Purchasing Security]

- Use a specific email account for all Internet purchases/transactions
- Use **strong and unique** passwords for all accounts
- **Only** use a dedicated credit card with fraud protection
- Consider using “one-time” credit card numbers
- Beware of FREE credit reports
- Use a **secure** web browser and email client
- Don't give out any valid information via e-mail, Web or otherwise – *fake it when you can!*



[E-mail Security]

- ***Don't unsubscribe!***
- Watch for **phishing and spam** and other scams; **report it!**
- Trust no one – *yes, this means even your friends and family*
- Learn attachment types such as exe, com, bat, vbs, scr, cpl...
- HTML mail vs. Text mail
- Choose your email client wisely
- Concerned? – *Just don't open it!*



[A Phishing Tale]

A True Story...

- User goes to health information website
- Health info website is compromised by hackers
- Hackers had placed malicious code on website
- Malicious code installs on computer and downloads more malicious code from other hacked web servers
- Keystroke logger is installed
- Passwords/account information keystrokes recorded
- All information is sent to Russia, China and Malaysia for use in fraudulent activity

Break

***More phishing after a
15 minute break...***

[A Phishing Tail...]

- Can look very real; highly deceptive
- Preys on emotion of some kind
- Usually time-sensitive; urgent
- Ghosting
- Seeding
- Web browsers aren't helping
- Essentially a form of social engineering

[Truth About Phishing]

- Banks will **never, ever, ever** email you asking for your account or personal information
- Nobody else will either; they all agree its a bad idea
- Look for mis-spellings and strange grammar
- Watch out for images vs. links
- Domain name hijacking and other trickery
- DNS spoofing and poisoning
- View the HTML source and look for strange URLs
- Examine any pop-ups for trusted names
- Cross-site scripting (XSS)
- Getting extremely sophisticated and hard to detect

[ID Theft Quiz]

1. The most common form of identity fraud is:

- A. Phone Fraud
- B. Credit Card Fraud
- C. Bank Fraud
- D. Loan Fraud

2. If you don't report your debit card lost or stolen until after 2 days, you are responsible for fraudulent charges up to:

- A. \$50
- B. \$100
- C. \$250
- D. \$500

3. How many credit bureaus/reporting agencies are there?

- A. 1
- B. 2
- C. 3
- D. 4

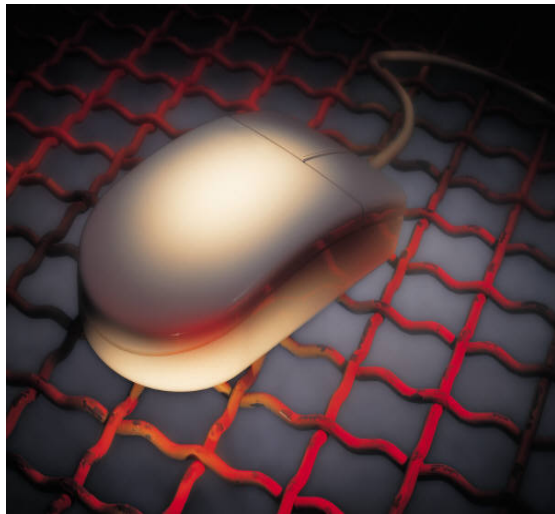
4. You should review your credit report every:

- A. Year
- B. 3 Years
- C. 5 Years
- D. 10 Years

[ID Theft Quiz (continued)]

5. The term Phishing refers to: Internet fraud/trickery for personal info
6. Whom do you contact when your identity has been stolen?
A. The Federal Trade Commission
B. Your employer
C. Your insurance agent
D. Your local grocer
7. The second most common form of identity fraud is:
A. Bank fraud
B. Mail fraud
C. Phone and Utilities fraud
D. Computer fraud
8. The term Spyware refers to: surreptitious monitoring software
9. How many people per minute are victims of identity theft.
A. 9
B. 13
C. 19
D. 23

[Web Browser Security]



Note: consider a browser such as Firefox or Opera,

Note: switch to Mac or Linux (or anyone who takes security seriously)

- You can ***easily*** be hacked through your web browser – ***very easily***
- Don't click "OK/Yes" on any prompt without reading it very carefully
- Don't click inside pop-ups if possible, use "Alt+F4" ("Alt+Tab" to pop-unders...)
- Clean out personal info (cookies, etc) often (weekly/monthly); you can be selective
- Do not allow browser to store passwords
- Ensure the "padlock" is visible in the system tray before entering any sensitive information

[Secure Deletion]

- Donating a system to charity?
- Giving your old system to a friend?
- Throwing away an old hard drive?

- **Deleting doesn't erase**
- ***Scrub the data!***
 - EraserD
 - Boot-n-Nuke

- Don't forget all media types
 - *Flash, USB, CDs, DVDs and Floppies count too!*

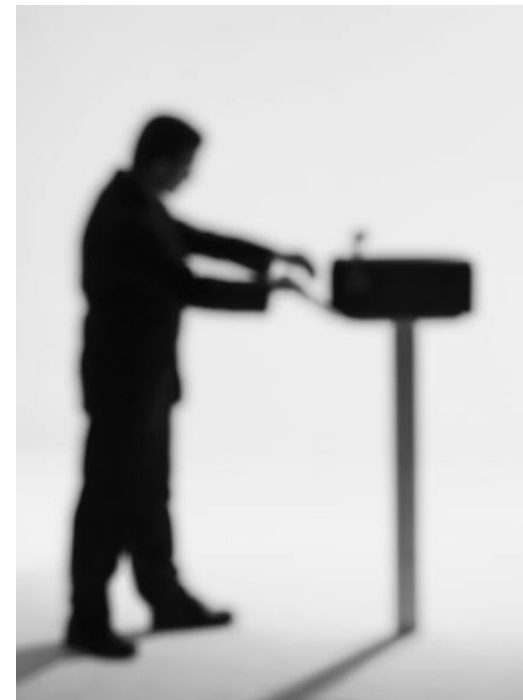


[Network Security Checklist]

- Use a hardware firewall
- Use a software firewall (w/IDS)
- Patch, patch, patch - automatically...
- Use anti-virus – and keep it updated (or auto-update **daily**)
- Use a spyware/adware blocker
- Harden operating system
 - Don't use Admin account by default; assign specific users
 - Strong passwords; upper and lower case, numbers, special characters
 - Disable unnecessary services
- Test your system periodically
 - Microsoft Baseline Security Analyzer
 - GRC – Shields Up!
- Configure wireless to be “secure”
 - Strong WEP key, at a minimum
 - MAC address restrictions
 - *“Wardriving” really does happen!*

["Snail Mail" Security]

- Don't leave mail in mailbox for long periods of time
- Lock your mailbox if you can
- Have the post office hold your mail when you go on vacation
- Pay online or direct debit/deposit if you can
- Shred all sensitive information with a **cross-cut shredder**
- Request non-SSN unique identifiers for all bills
- Change of address form; every 6 months if possible



[Telephone Security]

Cord vs. Cordless phones...

- Encrypted handset-to-base is the only secure cordless phone
- Wireless/cordless traffic is easy to “scan”
- Digit grabbers capture touchpad entries
- Lock your Demarcation box



Mobile/Cell phones...

- Mobile/cell traffic can be intercepted
- Bluetooth issues for mobile/cell phones
 - Viruses, DoS, Cross-talk
 - War-nibbling, Snarfing

Tip: Watch out for phone scams such as “yes/no”, phone phishing and unprotected voicemail...

Credit Card Security

- To sign, or not to sign?
- Write down all toll free numbers
- Handle credit card receipts carefully – just like cash (do not throw away!)
- Shred all pre-approved offers
- Shred all unused credit card checks
- Shred anything with account your info/number on it
- Shred old/unused cards



Tip: photocopy all items in your wallet and keep on file...

[Reduce Your Risk At Work]

- Do not print personal info and let it sit at the printer
- Be aware of your surroundings when ordering merchandise over the phone
- Do not store personal information on your desktop computer
- Put outgoing mail into secured mail boxes
- Do not leave benefit info (401K, etc) in your office



[What To Do If You're a Victim]

- **Contact all creditors – immediately!**
 - Change account information/number
 - Remove SSN as identifier
 - Establish a password, if possible
- Contact Credit Bureaus/Reporting Agencies and place a **Fraud Alert** on your account
 - Experian, Equifax, Trans Union
- Contact Federal agencies
 - Federal Trade Commission, Social Security Administration, Federal Bureau of Investigation, Secret Service, etc...
- Contact State Police
- Contact Local Police
- Contact your Legislators
- **Monitor all accounts very closely (daily)**
- **Quickly** challenge any newly discovered fraud



[What To Do If You're a Victim]

Create a checklist and log --

- Document all agencies/companies contacted
- Document exactly what they are going to do to remedy your issue and when they expect to have it done (verify)
- Get name of contact person you speak with *every time you call* – it may change
- Record every phone number you call and if you get transferred, write down the new number
- Record time and duration of calls
- Take extensive notes or record conversation
- ***Be persistent!*** Ask to speak with a supervisor. Don't take "no" for an answer unless you absolutely must

Get protection (if it is bad enough)

- Seek legal help
- Seek organizations like **LifeLock**



[ID Theft/Fraud Resources]

- **Experian (formerly TRW)**
 - www.experian.com
 - General Number and Fraud Line: 888.397.3742
- **Equifax**
 - www.equifax.com
 - General Number: 800.685.1111
 - Fraud Line: 800.525.6285
- **Trans Union**
 - www.transunion.com
 - General Number: 800.916.8800
 - Fraud Line: 800.680.7289
- **Social Security Administration**
 - www.ssa.gov/oig/public_fraud_reporting/index.htm
 - 800.269.0271
- **Federal Trade Commission**
 - www.consumer.gov/idtheft
 - 1.877.IDTHEFT (438.4338)
- **Federal Bureau of Investigation**
 - www.fbi.gov
 - www.ifccfbi.gov

[ID Theft/Fraud Resources]

- www.OnGuardOnline.gov – report Internet fraud to the FTC
- dunsapp.usps.gov/HoldMail.jsp - link to hold mail
- www.usps.gov/websites/depart/inspect - report stolen mail
- **Secret Service**
 - www.ustreas.gov/usss
 - www.secretservice.gov/field_offices.shtml
- **Do Not Call Registry:**
 - donotcall.gov
 - 888.382.1222 (stops telemarketers from calling)
- **Annual Credit Report:**
 - www.annualcreditreport.com
 - 888.322.8228
- **Report stolen checks to:**
 - SCAN: 800.262.7771
 - TeleCheck: 800.710.9898 or 800.927.0188
 - Equifax Check Systems: 800.437.5120
- **Stop credit card solicitation:**
 - 888.567.8688 (stops credit bureaus from selling your name for 2 years)

[ID Theft/Fraud Resources]

- www.staysafeonline.org – National Cyber Security Alliance
- www.FightIDTheft.com – excellent resource for victims
- www.getnetwise.com – get security-smart about the ‘net
- www.phishreport.net – Symantec’s anti-phishing site
- www.antiphishing.org – excellent resource for fighting phishing
- reportphishing@antiphishing.org – report phishing
- spam@uce.gov – report spam
- www.419eater.com/ - take on the scammers if you dare
- survey.mailfrontier.com/survey/quiztest.html – phishing test
- www.netriplex.com/phishfraud/phishing_test.aspx - phishing test
- www.lifelock.com – proactive ID protection (for a fee)
- darrel.knutson.com/english_educ/english-acronyms.html – great resource for breaking the kids online code
- **Tom Liston’s “Follow the Bounding Malware”** –
 - Chapter 1: <http://isc.sans.org/diary.php?date=2004-07-23>
 - Chapter 2: <http://isc.sans.org/diary.php?date=2004-08-23>
 - Chapter 3: <http://isc.sans.org/diary.php?storyid=355>

[ID Theft/Fraud Resources]

- **Portland Police Bureau**
 - www.portlandonline.com/police/
- **Vancouver Police**
 - www.ci.vancouver.wa.us/police.asp?menuid=10465&submenuid=10527
- **Oregon State Police**
 - www.osp.state.or.us
- **Washington State Police**
 - www.wsp.wa.gov
- **Oregon Legislators**
 - www.leg.state.or.us/findlegsltr/findset.htm
- **Washington Legislators**
 - www1.leg.wa.gov/legislature

Info-Security Resources

- **US CERT** – US Computer Emergency Response Team
 - <http://www.us-cert.gov/>
- **The I3P** – Security in the News
 - <http://www.thei3p.org/news/today.html>
- **DHS Daily Report** - Department of Homeland Security daily report
 - <http://www.nipc.gov/dailyreports/dailyindex.htm>
- **SANS Internet Storm Center** - Internet “weather report”; highly recommended reading on a daily basis
 - <http://www.incidents.org>
- **Secunia** - Comprehensive list of all known vulnerabilities
 - <http://www.secunia.com>
- **Security Tracker** - Comprehensive list of all known vulnerabilities
 - <http://www.securitytracker.com>
- **Security Focus**
 - <http://www.securityfocus.com>
- **Bruce Schneier** – Information Security author and luminary; read the blog
 - www.schneier.com
- **Gibson Research Corp** - Security tools and external testing/scanning
 - <http://www.grc.com>
- **Robert Graham** - Expert security dictionary and information resource
 - <http://www.robertgraham.com>

Security Product Resources

- **RealSecure (BlackICE)** - Personal firewall & intrusion detection system
 - http://blackice.iss.net/product_pc_protection.php
- **ZoneAlarm** - Personal firewall, spam filter, pop-up blocker
 - <http://www.zonelabs.com/store/content/home.jsp>
- **AVG** – FREE Antivirus product
 - <http://free.grisoft.com/>
- **TrendMicro** - Antivirus product
 - <http://www.trendmicro.com/en/home/us/enterprise.htm>
- **F-Secure** - Antivirus product
 - <http://www.f-secure.com/>
- **Symantec** - Antivirus product
 - http://www.symantec.com/product/index_homecomp.html
- **Mozilla Firefox** – excellent alternative browser
 - <http://www.getfirefox.com>
- **Opera** – another excellent alternative browser
 - <http://www.opera.com>
- **PasswordSafe** – Store all passwords securely inside a password safe
 - <http://www.counterpane.com/passsafe.html>
- **ACrypt** - Easy to use encryption program
 - <http://www.acrypt.com/>
- **PGP** - Powerful [but relatively complex] encryption program
 - <http://www.pgp.com>
- **EraserD** - File shredder, secure deletion program
 - <http://download.sourceforge.net/eraser/eraser53s.zip>
- **Boot-n-Nuke** – Disk eraser
 - <http://dban.sourceforge.net/>

Microsoft Security Resources

- **Microsoft Update Center**
 - <http://windowsupdate.microsoft.com/>
- **Microsoft Security Center**
 - <http://www.microsoft.com/security/>
- **Microsoft Office Updates**
 - <http://office.microsoft.com/productupdates>
- **Microsoft Security Bulletin Service**
 - <http://www.microsoft.com/technet/security/bulletin/notify.asp>
- **Microsoft Security Tools and Checklists**
 - <http://www.microsoft.com/technet/security/tools/tools.asp>
- **Microsoft Baseline Security Analyzer**
 - <http://www.microsoft.com/technet/security/tools/tools/MBSAHome.ASP>
- **Microsoft HFNetCheck**
 - <http://www.microsoft.com/technet/security/tools/tools/hfnetchk.asp>

[Questions?]

Patrick C. Miller

CISA CISSP-ISSAP SSCP NSA-IAM TCP

patrick@pcmill.com

503.312.0703

<http://www.pcmill.com/presentations/>