

Protecting your Personal Information

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

Stoel Rives, Attorneys at Law – March 21st 2006

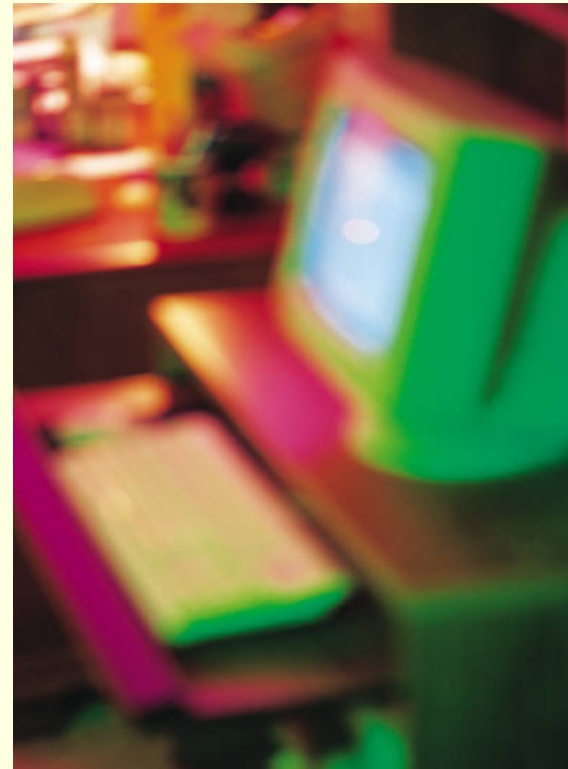
Introduction

Why trust me?

- More than 20 years experience in general IT
- Sr. Information Security Consultant - more than 9 years experience in Information Security
- 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, rootkits and spyware – oh my!



The Current Situation

- 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
- Importance/Herd Factor misconception
- ID Theft – **FBI/SS #1 crime** – very real threat...
- Federal (and State) Agencies are passing the buck

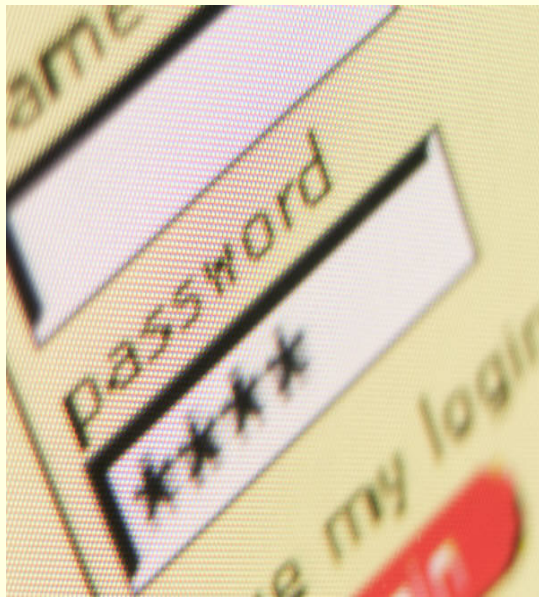


Why Should You Protect Your Personal Information?

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 systems
- Loss of job if your home computer is found to be the source of a corporate security breach
- Loss of reputation, even if wrongfully accused
- Many “intangibles” – more than you can imagine until you’ve actually been there
- ***You may receive criminal treatment and investigation for crimes committed using your ID, systems or network space!***

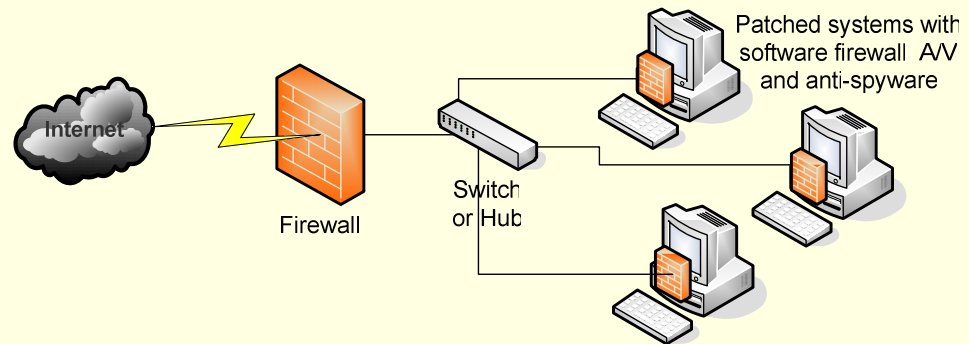
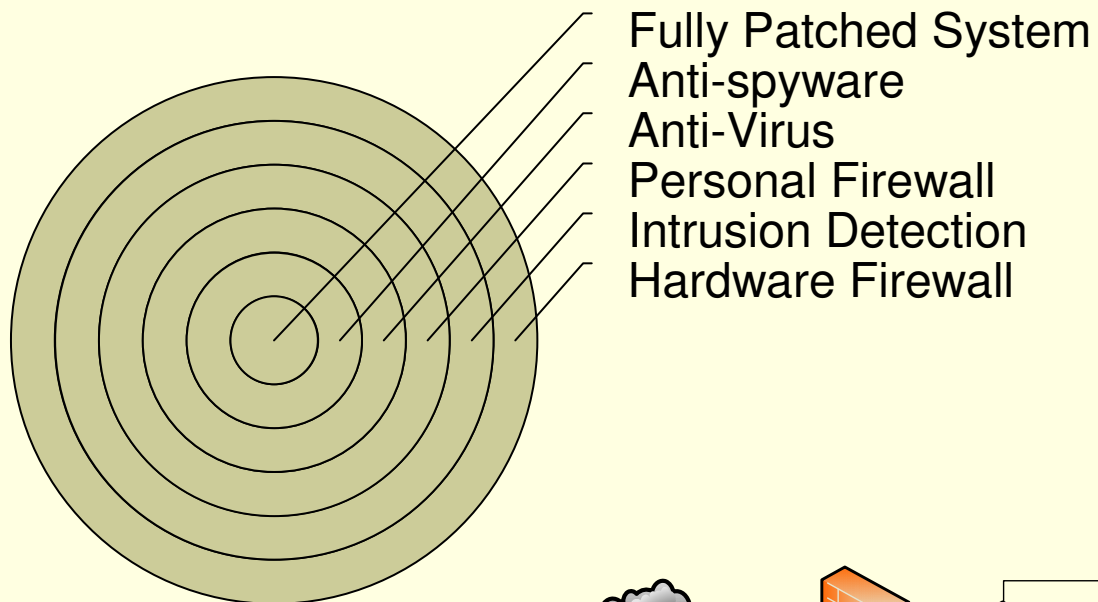
Electronic Information Security



Defense in depth!

- Protection Hardware
- Protection Software
- **Patch, patch, patch!**
- Use *strong and unique* passwords
- Encrypt where feasible

The Layered (Fortress) Model



Protection Hardware

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

- *Wireless can be very dangerous if not used correctly...*



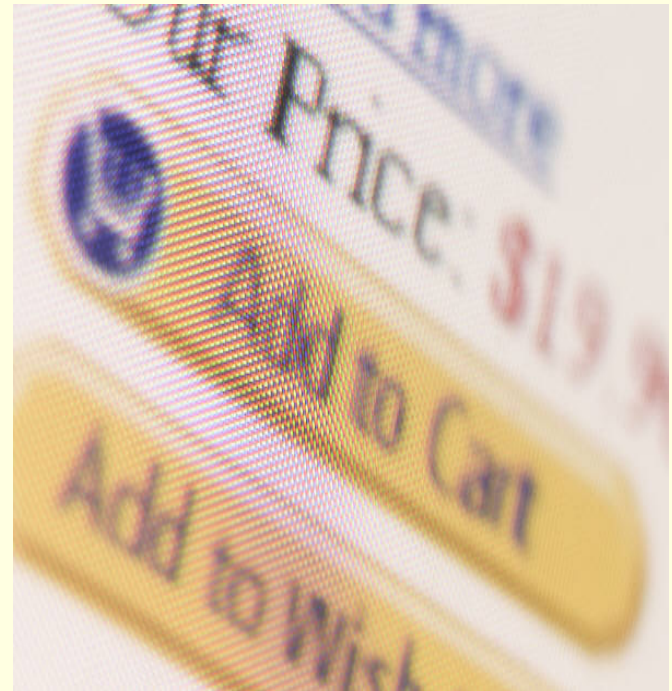
Protection Software



- 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...

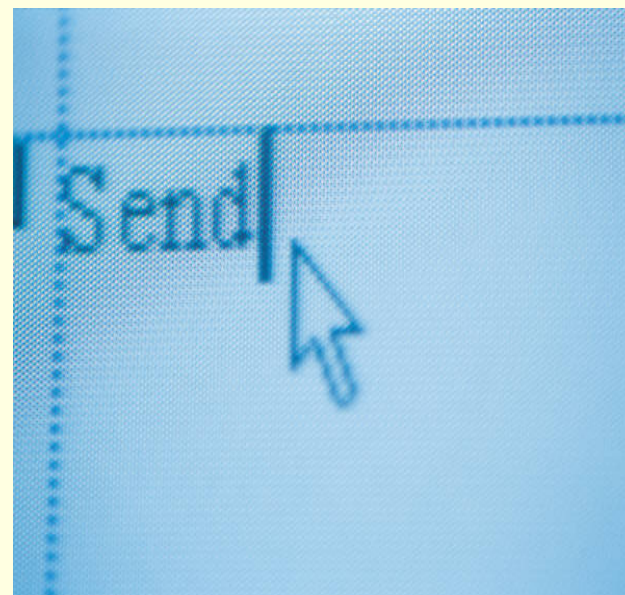
Internet Purchasing Security

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

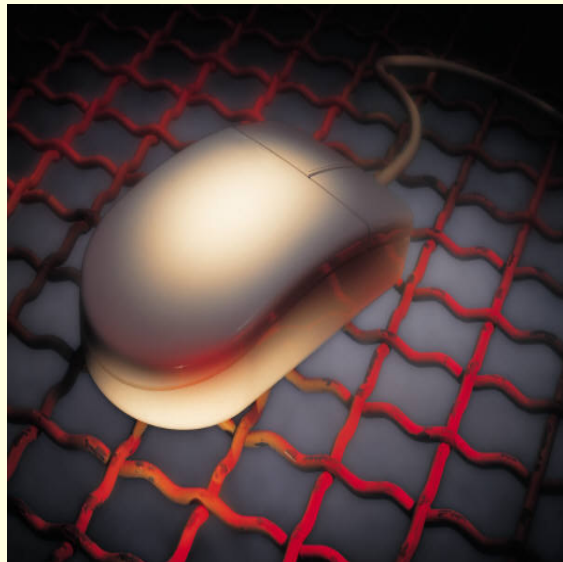


E-mail Security

- **Don't unsubscribe** to spam
- Watch for “**phishing**” and other online scams (phishing test)
 - Banks will **never** email you asking for your credentials
 - Mis-spellings, strange grammar
 - Images vs. links
 - Domain name tricks, XSS
 - Take the Phishing tests...
- Trust no one – *yes, this means even your friends and family*
- Learn attachment types (exe, com, bat)
- Beware of HTML mail...
- Concerned? – Just don't open it!



Web Browser Security



- You can **easily** be hacked through your web browser – *biggest current e-threat*
- 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 Cookies 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
- Consider an "alternate" browser such as Mozilla, Opera, etc...

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!*

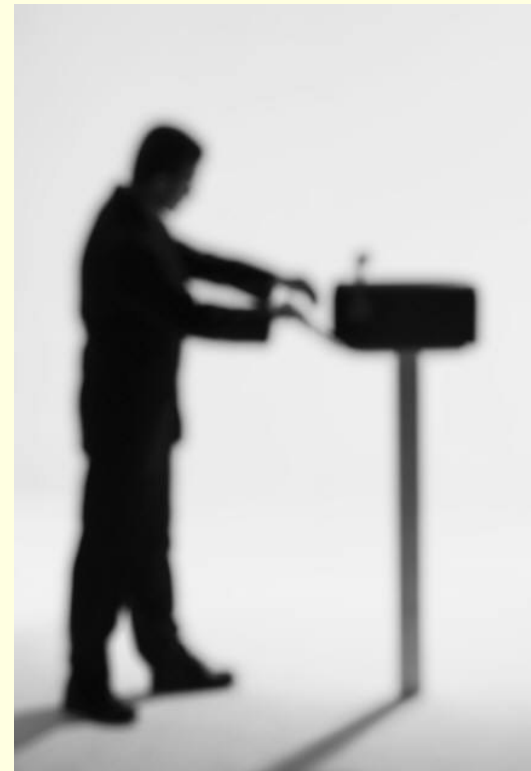


Home Network Security Checklist

- 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** – *even free offers*
- Request non-SSN unique identifiers for all bills
- Periodic change of address form, just to be safe



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
(phone phishing)!***

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 info/number
- 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 and get a **Fraud Alert** put on your account
 - Experian, Equifax, Trans Union
- Contact Federal agencies
 - Social Security Administration, Federal Bureau of Investigation, Federal Trade Commission, 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 and 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 and Fraud Resources

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

ID Theft and Fraud Resources

- <http://www.OnGuardOnline.gov> – report Internet fraud to the FTC
- <http://www.FightIDTheft.com> – excellent resource for victims
- <http://www.lifelock.com> – proactive ID protection (for a fee)
- <https://dunsapp.usps.gov/HoldMail.jsp> - link to hold mail
- <http://www.usps.gov/websites/depart/inspect> - report stolen mail
- spam@uce.gov – report spam
- reportphishing@antiphishing.org – report phishing
- **Do Not Call Registry:**
 - <http://donotcall.gov>
 - 888.382.1222 (stops telemarketers from calling)
- **Annual Credit Report:**
 - <http://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 and Fraud Resources

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

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/>

Security Information 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.nipcr.gov/dailyreports/dailyindex.htm>
- **SANS Internet Storm Center** - Internet “weather report”; highly recommended
 - <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>
- **World Virus Map** - Interactive map of all current viruses
 - <http://www.trendmicro.com/map>
- **Security Focus**
 - <http://www.securityfocus.com>
- **Gibson Research Corp** - Security tools and external testing/scanning
 - <http://www.grc.com>
- **Robert Graham** - Expert security lexicon/dictionary and information resource
 - <http://www.robertgraham.com>
- **Phishing Tests** – Sites to test your Phishing detection skills
 - <http://survey.mailfrontier.com/survey/quiztest.html>
 - http://www.netriplex.com/phishfraud/phishing_test.aspx

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

patrick@pcmill.com

503.312.0703

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