

PERSONAL INFORMATION PROTECTION



Minimizing your potential for fraud and ID theft
& what to do if it happens to you

Employee Assistance Program
Reed College, 04-20-2005

Given by: Patrick C Miller CISSP-ISSAP SSCP NSA-IAM



Introduction

Why trust me?

- More than 18 years experience in general IT
- Senior Information Security Consultant - more than 7 years experience in Information Security
- Industry certified
 - CISSP-ISSAP
 - SSCP
 - NSA-IAM
 - TCP, *etc.*
- **I have been a victim of ID theft myself...**

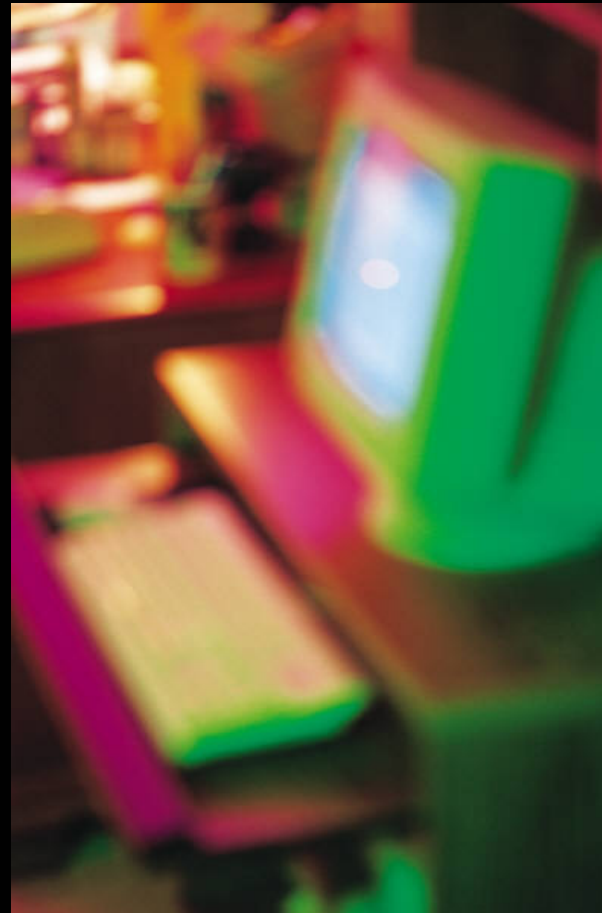
The Current Situation

- ID Theft – **FBI/SS #1 crime** – very real threat...
- Federal (and State) Agencies are passing the buck
- Importance/Herd Factor misconception – there is diminishing safety in numbers (automated scans and mass-mailers will find you)
- Point-and-click tools for scanning and hacking systems are freely available on the Internet – skill is not required



The Current Situation

- General weak information security practices everywhere
- The Internet is **not** the most common vector – physical theft is a greater risk – for now...
- Organized crime “cookbooks”
- Hackers, criminals and even terrorists are actively looking for vulnerable systems to use
- Watch out for “snake-oil”



Why Should You Protect Your Personal Information?

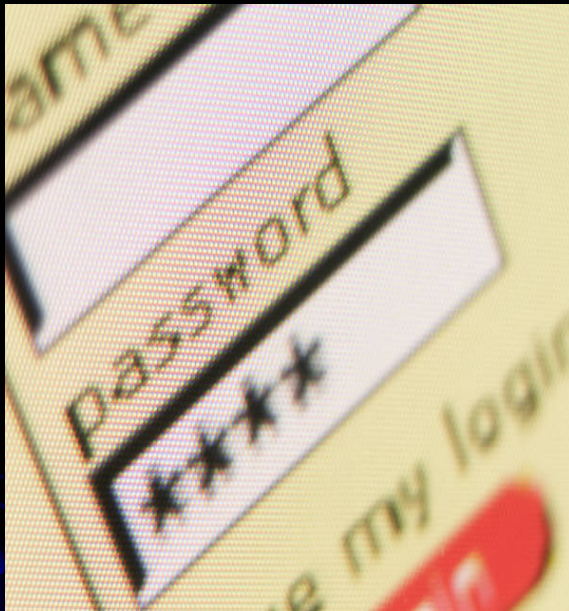
Impacts associated with ID Theft...

- Loss of funds
- Negative 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
- *You may receive criminal treatment and investigation for crimes committed from your systems or network space*

100% Security vs. Reality

- No “Silver Bullet”
- Requires constant vigilance
- Nothing is truly “Secure”
- Security is not obscurity
- Tradeoff of functionality/convenience
- More security = higher cost at a higher level of complexity
- You don't have to “outrun the bear”

Electronic Information Security



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

Protection Software



- Personal Firewalls
- Anti-Virus
- Spyware/Adware Blockers
- Others...
 - Content filters
 - Pop-up blockers
 - Cookie crushers
 - History scrubbers
- All-in-one packages
- Encryption...

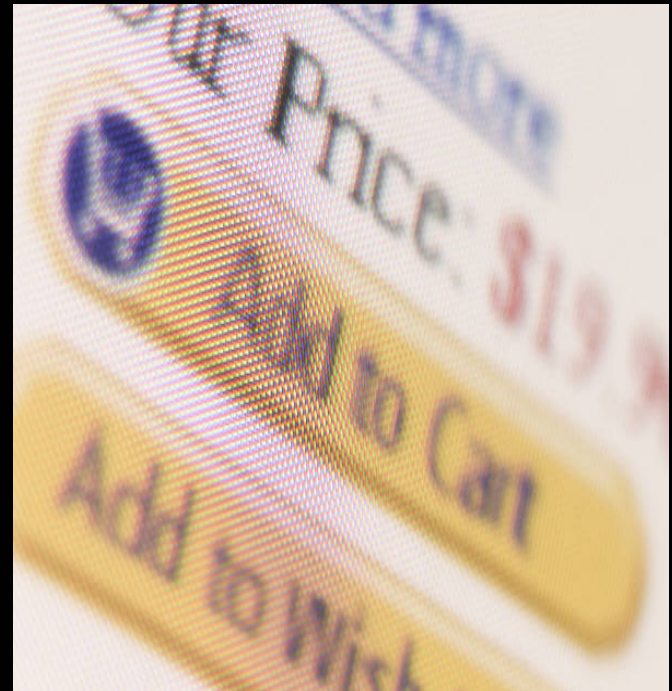
Protection Hardware

- Hardware Firewalls
 - Routers/Modems
 - VPN
- USB tokens
- SecurID
- Biometrics
- *Wireless can be dangerous if not used correctly...*



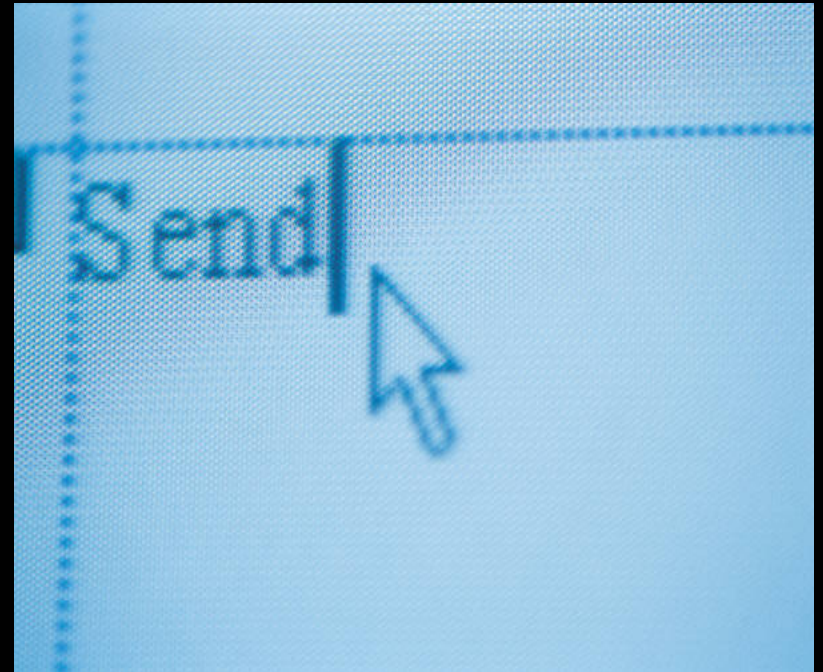
Internet Purchasing Security

- Get a “webmail” (or otherwise separate) account for all personal Internet transactions
- Use a strong *and unique* password 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*

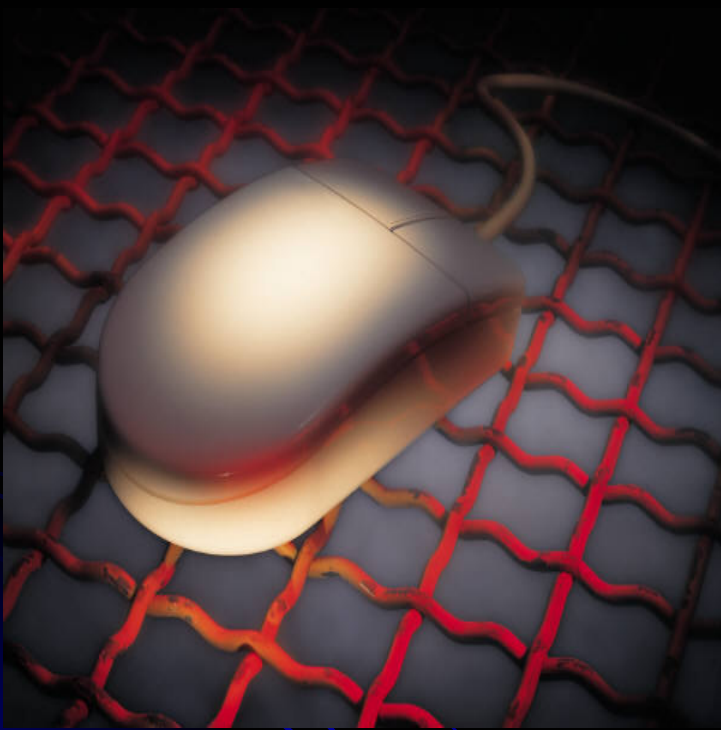


E-mail Security

- Use special/restricted account for financial activity
- **Don't unsubscribe** to spam
- Watch for “**phishing**” and other online scams
 - Microsoft, Paypal, eBay, banks etc will **never** email you asking for your credentials
 - Mis-spellings, strange grammar
 - Images vs. links
 - Domain name tricks
 - Take the Phishing tests...
- Trust no one – even friends/family
- Learn attachment types
(* .exe, * .zip, * .com, * .bat, * .scr)
- Concerned? – Just don't open it!



Web Browser Security



- You can *easily* be hacked through your web browser – quickly becoming most common threat vector...
- Don't click "OK/Yes" on any prompt without reading it very carefully
- Don't click inside pop-ups, use "Alt+F4" ("Alt+Tab" to pop-unders...)
- Clean out Cookies regularly (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...

Encryption



- Password Safes (Counterpane)
 - Store all passwords in one safe location accessed by a single password
 - Hold multiple safes in one application
- File encryption (ACrypt, PGP)
 - Encrypt specific files
 - Encrypt entire drives or partitions
- Email encryption (PGP)
 - Encrypt content attached to email
 - Encrypt entire email - text and all

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

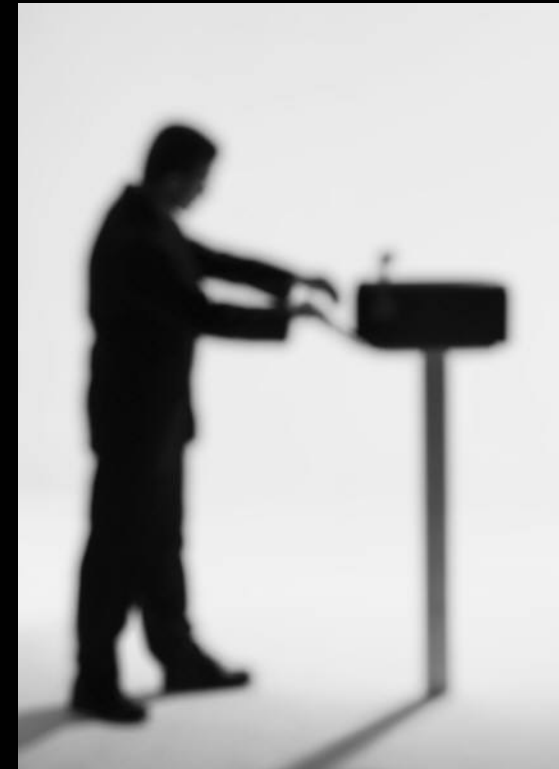


Home Network Security Checklist

- Use a hardware firewall
- Use a software firewall (w/IDS)
- Patch, patch, patch - automatically...
- Use anti-virus – and keep it updated (or auto-update)
- 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
 - MAC address restrictions
 - “Wardriving” happens...

“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



Check Security

- Use initials on checks instead of first name
- Only use the last 4 digits of your credit card number in the “For/Memo” space to pay checks to credit card company
- **Never** put your SSN on your checks
- Shred any voided check

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

Jane Doe 101 Anydrive Hometown, IN 46278	FRN (Fractional Routing Number) → 12-345/678 - OR - 12-3456 789	5600
PAY TO THE ORDER OF		DATE
MEMO		\$ <input type="text"/>
123456789 123456789101112 5600		DOLLARS
		SIGNATURE

Credit Card Security

- Write down all toll free numbers
- Don't sign credit cards, use "PHOTO ID REQUIRED" instead
- Handle credit card receipts carefully – like cash
- Shred all pre-approved offers
- Shred all unused credit card checks
- Shred anything with account info/number



Telephone Security



Cord vs. Cordless phones...

- Encrypted handset-to-base is the only secure cordless (*not* cell/mobile) 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

***Watch out for phone scams
(phone phishing)***

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 Oregon State Police**
- **Contact local Police**
- **Contact your Legislators**
- **Monitor all accounts very closely (daily)**



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



Fraud Reporting Resources

- **Experian (formerly TRW)**
 - <http://www.experian.com> – 888.397.3742
- **Equifax**
 - <http://www.equifax.com> – 800.525.6285
- **Trans Union**
 - <http://www.transunion.com> – 800.680.7289
- **Social Security Administration**
 - <http://www.consumer.gov/idtheft/> – 800.269.0271
- **Federal Trade Commission**
 - [https://rn.ftc.gov/pls/dod/widtpubl\\$.startup?Z_ORG_CODE=PU03](https://rn.ftc.gov/pls/dod/widtpubl$.startup?Z_ORG_CODE=PU03) – 1.877.IDTHEFT (438.4338)
- **Federal Bureau of Investigation**
 - <http://www.fbi.gov>
- **Secret Service**
 - <http://www.ustreas.gov/usss>
- **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>

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**
 - [www.microsoft.com/technet/security/ tools/tools/MBSAHome.ASP](http://www.microsoft.com/technet/security/tools/tools/MBSAHome.ASP)
- **Microsoft HFNetCheck**
 - <http://www.microsoft.com/technet/security/tools/tools/hfnetchk.asp>

Other Security 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
- **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/>

Other Security Resources

- **USPS** – US Post Office
 - <http://www.usps.gov/>
- **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”
 - <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

Questions?

Patrick C. Miller

CISSP-ISSAP SSCP NSA-IAM

patrick@pcmill.com

503.312.0703

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

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