



# Agenda

---

- Protecting Against
  - Identity Theft
  - Buying Online
  - Viruses
  - Social Engineering
  - Hoaxes, Virus Myths, and Scams
  - Spyware
- What we're doing at MCG

# Identity Theft

---

- Nationally, about 7 million consumers became victims of identity theft during 2002
- According to 2 studies done in July 2003 (Gartner Research and Harris Interactive)
  - approximately 7 million people became victims of identity theft in the prior 12 months.
    - 19,178 per day
    - 799 per hour
    - 13.3 per minute.
- The incidence of victimization increased
  - 11-20% between 2001-2002
  - 80% between 2002 -2003 (Harris Interactive).

# Identity Theft

---

- Victims now spend an average of 600 hours recovering from this crime, often over a period of years.
- Three years ago the average was 175 hours of time, representing an increase of about 2470%.
- Based on 600 hours times the indicated victim wages, this equals nearly \$16,000 in lost potential or realized income.
- Victims spend an average of \$1,400 in out-of-pocket expenses, an increase of 85% from years past.
- While victims are finding out about the crime more quickly, it is taking far longer than ever before to clear their records and recover from the situation.

# Identity Theft

---

- Approximately 85% of victims found out about the crime due to an adverse situation:
  - denied credit or employment
  - notification by police or collection agencies
  - receipt of credit cards bills never ordered.
  - Only 15% found out through a positive action taken by a business group that verified a submitted application or a reported change of address.



# Identity Theft

---

- Even after the thief stops using the information, victims struggle with the impact of identity theft.
- That might include:
  - increased insurance or credit card fees
  - inability to find a job
  - higher interest rates
  - battling collection agencies
  - and issuers who refuse to clear records despite substantiating evidence of the crime.
- This "tale" may continue for more than 10 years after the crime was first discovered.



# Information important to an identity thief

---

- Zip code
- Driver's license
- Home address
- Phone Number
- PIN
- Credit card numbers
- SSN
- Passports

# Examples of Identity Theft

---

## Examples:

- **Purse snatching.** A thief steals your wallet or purse containing your ID and credit and bankcards.
- **Mail theft.** Thieves steal bank and credit card statements, pre-approved credit offers, telephone calling cards and tax information from your mailbox.
- **Change of address.** Thieves divert your mail to another location.
- **Dumpster diving.** Thieves rummage through residential or business trash, looking for personal information.
- **Masquerading.** Thieves fraudulently pose as your employer, landlord or someone else with a legitimate need for your personal information.



# Examples of Identity Theft

---

- **Stealing work records.** Thieves get your business or personnel records at work.
- **Home theft.** Thieves find personal information in your home.
- **Internet theft.** Thieves obtain personal information from unsecured Web sites that you may have visited.
- **Insider crime.** People who have access to personal identifying information steal it to use themselves or to sell to other thieves.
- **Pretexting.** Thieves pretend to be you or a legitimate requestor and persuade business employees to provide them with your personal information.
- **Corporate espionage.** Thieves steal business secrets such as new product plans or bidding strategy.

# What thieves do with your personal information:

---

- **Contact your creditors**, gain access to your accounts, change mailing addresses and begin using the accounts.
- **Open new credit** or bank accounts, obtain loans and establish phone and utility service fraudulently using your name, Social Security number and birth date.
- **File bankruptcy under your name** to avoid paying debts they falsely incurred or to avoid eviction.
- **Counterfeit checks or debit cards** and drain your bank account.
- **File fraudulent tax returns.**
- **Obtain driver's licenses and other fake identification documents.**
- **Use insurance information to obtain medical procedures.**
- **Buy cars or houses** taking out loans in your name.
- **Sell business information to competitors.**



# What To Do?

---

- Shred everything with personal information on it
- Cut up cards
- Do not give away personal information to anyone
- Do not respond to ANY Email message with personal information
- Be Skeptical
- Never use a public computer for secure computing.



# Red Flags for Internet Users

---

- Email asking for personal information
- Email asking for any information that you've already given
- Website or Email with a different domain than what you typically use
- Non-secure input form
- No authentication requirement
- Claim of lost or "flushed" information

# Tips

---

- Never give out SSN online – unless sure of source.
- Never give out your bank or credit card number – unless setting up online banking
- Sanitize online resumes
- Look for misspellings or bad grammar on the website.
- Opt out of websites that offer public information on you.

# Tips

---

- Remove your email and snail-mail addresses from direct-marketing lists at the Direct Marketing Association's website (<http://the-dma.org>).
- Limit the amount of information you share.
- Treat all requests as hostile – especially when SSN is needed
- Bank Online
- Direct your bills to an online bill paying service (i.e. PayPal, PayTrust, etc)



# Protect Yourself

---

- Put your SS card in a safe, secure place.
- Have your SSN removed from your driver's license.
- Opt of pre-approved credit card offers (888-5-OPTOUT)
- Secure your mailbox
- Consider shredding



# Order a copy of your credit report

---

Credit report contains:

- Names of your creditors
- Account numbers
- When the accounts were opened
- Your balance
- Timely payments?
- Where you work and live
- If you've been sued, arrested, or filed bankruptcy.



# Credit Bureaus

---

- Equifax Credit Information
  - [www.equifax.com](http://www.equifax.com)
- Experian Information Solutions
  - [www.experian.com](http://www.experian.com)
- TransUnion
  - [www.transunion.com](http://www.transunion.com)



# Credit Monitoring Services

---

- TrueCredit.com
  - Charges between \$35-\$80 per year.
  - Weekly emails point out status changes
    - New lines of credit in your name
    - Inquiries by others on your credit
    - Address changes filed



Awareness of the danger of  
identity theft is your best defense.

---

Pay attention when you're asked for  
information.



# Buying Online

---

Is it Safe?

Yes...

If you pay attention and proceed with caution



# Tips

---

- Never buy from spammers
- Look critically at the website
- Think about the price



# Internet Auctions

---

- \$7 billion in sales per year
- Gigantic garage sale
- Consider escrow for expensive purchases ([www.escrow.com](http://www.escrow.com))
- Always use credit card
- Never use debit card



# Internet Auctions

---

- Ask the seller for a telephone number
- Follow the site's advice
- Ask the seller how they acquired the merchandise
- If it's too good to be true...it probably is.
- Never deal with someone outside of the auction floor.
- If you feel you are being ripped off, complain.



# Viruses

---

Computer code that modifies other programs when they are executed.

# Viruses

---

- It must be executed before it can do damage – most of the time.
- Most common ways viruses spread are:
  - Double clicking attachments
  - Visiting websites designed to execute a command.
  - Opening an infected email message in preview mode.



# Virus Dictionary

---

- Malicious code: any computer code that can do damage or negatively impact a computer.
- Virus: a program that infects a computer and modifies other programs.
- Worm: a type of virus that can spread without infecting a specific program or file.
- AV Scanner: Antivirus scanner or program.



# Virus Dictionary

---

- Virus definitions: database of known viruses.
- Vulnerability: Any mistake or feature set that gives the hacker or virus unauthorized access to the computer.
- Backdoor trojans: Programs that hide on your computer, trying to evade detection while they perform unauthorized actions.
- Key loggers: Programs that record mouse clicks, keystrokes, and sometimes screen shots of your computer activity.
- SMTP engine: an email program that can send files without using programs installed on your computer.



# Virus Free

---

- Always run AV software
- Always keep it up-to-date
- Always scan regularly
- Always keep your system and software up-to-date with the latest patches and service packs.



# Virus Free

---

- Never download software from suspicious sites
- Never open attachments from senders you do not know
- If the message appears suspicious, delete it.
- Turn off all unnecessary services in your operating system
- Learn to configure your web browser with appropriate security settings

# Internet Explorer Settings

---

## ○ Security Tab

- Download signed ActiveX controls: Prompt
- Download unsigned ActiveX controls: Disable
- Initialize and script ActiveX controls not marked as safe: Disable
- Run ActiveX controls and plug-ins: Enable
- Script ActiveX controls marked safe for scripting: Enable
- Downloads: Enable
- Font Download: Enable



# Internet Explorer Settings

---

- Java Permissions: High Safety
- Access data sources across domains: Disable
- Allow META REFRESH: Enable
- Display mixed content: Enable
- Don't prompt for client certificate selection when no certificates or only one certificate exists: Disable
- Drag and drop or copy and paste files: Enable
- Installation of desktop items: Prompt
- Launching of desktop items: Prompt



# Internet Explorer Settings

---

- Launching programs and files in an IFRAME: Prompt
- Navigate sub-frames across different domains: Prompt
- Software channel permissions: Medium Safety
- Submit non-encrypted form data: Enable
- Userdata persistence: Enable
- Active scripting: Enable
- Allow paste operations via script: Enable
- Scripting of Java applets: Prompt
- Logon: Prompt



# Social Engineering

---

Defined: obtaining confidential information by means of human interaction (Business Wire, August 4, 1998).



# Social Engineering

---

- Not a technology – exploits human weakness – carelessness or helpfulness.
- Specialized con-artists.
- Easiest way to gain unauthorized access to computer network.
- Most famous “social engineer” – Kevin Mitnick  
([www.zdnet.com/filters/printerfriendly/0,6061,2604480-2,00.html](http://www.zdnet.com/filters/printerfriendly/0,6061,2604480-2,00.html)).

# Social Engineering

---

- More information: *Everything You Wanted to Know about Social Engineering – But Were Afraid to Ask*, at Happy Hacker web site ([www.happyhacker.org/uberhacker/se.shtml](http://www.happyhacker.org/uberhacker/se.shtml)).
- Never share your password with anyone.
- Use STRONG passwords
- Change your password regularly
- Never write down your password
- Never send your password over the Internet
- Always ask for ID when someone is going to work on your computer.
- Store sensitive data on a secured network drive.



# Hoaxes, Virus Myths, and Scams

---



# Hoaxes, Virus Myths, and Scams

---

- Hoaxes are similar to prank phone calls and then forwarded by gullible computer users.
- Create Email bottlenecks and unnecessary traffic.
- Convince people to delete viable files from their computer.
- Some people have died falling for Internet scams.

# Hoaxes and Virus Myths

---

- Recognition
  - If you don't understand the jargon or the message is warning you about files in your computer you've never heard of – it's probably a hoax.
  - Subject line is in all CAPS
  - If it looks too good to be true, it probably is.
  - If it sounds too good to be true, it probably is.
  - If it is illegal, immoral, or unethical, you will probably be the loser.
- Check things out FIRST before you forward to your friends.
  - <http://www.symantec.com/avcenter/hoax.html>
  - <http://hoaxbusters.ciac.org/>
  - <http://vil.mcafee.com/hoax.asp>
  - <http://www.snopes.com/> (urban legends)

# Scams

---

- Nigerian Letter Scam (grand daddy of the all).
  - At least 17 people have died
  - Goto - <http://www.tip.net.au/spam/Nigerian-419-Scam.html> for the list of variations
  - Secret Service website reports 100 calls per day and 300-500 pieces of related messages per day.

# Advice

---

- Avoid Internet based investment opportunities – especially those that arrive through SPAM.
- SEC considers it a plague.
  - They've setup fake investment opportunity sites to educate the public
    - <http://www.mcwhortle.com/>
    - <http://www.growthventure.com/parsons>
    - Receives 150,000 hits in the first 3 days.



# Spyware

---

# Spyware

---

- **28**  
The average number of spyware programs on a personal computer, according to a report from EarthLink and WebRoot Software. Most of it was advertising related, the vendors said.  
**Source:** [TechWeb](#)
- **36.8 percent**  
The number of surveyed companies that had suffered one or more browser-based attacks in the last six months, up 25 percent from 2003, according to survey sponsor Computing Technology Industry Association.  
**Source:** [News.com](#)
- **40,000**  
The number of calls EarthLink fields each month from customers trying to discern if "phishing" e-mails are indeed from EarthLink.  
**Source:** [ITtoolbox.com](#)

# What is Spyware

---

1. **Spyware** is Internet jargon for **Advertising Supported software** (Adware). It is a way for shareware authors to make money from a product, other than by selling it to the users. There are several large media companies that offer them to place banner ads in their products in exchange for a portion of the revenue from banner sales. This way, you don't have to pay for the software and the developers are still getting paid. If you find the banners annoying, there is usually an option to remove them, by paying the regular licensing fee. (Source: [spychecker.com](http://spychecker.com))



# What is Spyware

---

- Spyware, sometimes called adware, snoopware or sneakware, is software that secretly gathers information about a user and relays that information to another party over the Internet. In many cases, users unknowingly install spyware when they download freeware or shareware, even though references -- often obscure -- to spyware might be included in the program's end-user agreement. In other instances, spyware programs are automatically installed when a user simply views an HTML e-mail or visits a certain Web page.
  - At its mildest, spyware is a simple tool used by advertisers to track users' Web-surfing preferences.
  - At its worst, spyware is used to monitor keystrokes, scan files, install additional spyware, reconfigure Web browsers, snoop e-mail and other applications, and more. Some of today's spyware can even capture screenshots or turn on webcams.

Source: Computerworld



# What Spyware does to you

---

1. Steal your Information (Identity Theft)
2. PopUp/Under Ads to you
3. SPAM Your Inbox
4. Slows down your computer
5. Crash your computer

Source: [spykiller.com](http://spykiller.com)

# What Spyware does to you

---

- Spyware also leads to spam and vice versa. When spyware finds e-mail addresses, it sends them back out over the Internet to be traded, shared or sold to spammers. When unsolicited commercial e-mail finds a user who clicks to see an advertised product, spyware secretly downloads as the advertisement unfolds. This creates an administrative nightmare for corporate IT professionals, not to mention the legal implications it introduces as inappropriate content floods in-boxes.

# What Spyware does to you

---

- Spyware also consumes memory and system resources. Because it constantly phones home to deliver user information and then sends back more pop-ups, banner ads and the like, spyware uses up valuable corporate bandwidth. Also, many spyware programs store their unwanted advertisements on the user's own hard drive.
- Perhaps one of the biggest concerns regarding spyware in the corporation is the challenge it presents to organizations struggling to demonstrate compliance with government regulations for information security. While many of these regulations target specific industries, few corporate environments are unaffected. These regulations include the Health Insurance Portability and Accountability Act, established to ensure the privacy of patient information; the Sarbanes-Oxley Act, established to ensure that financial statements are resistant to fraud; the Gramm-Leach-Bliley Act, established to safeguard customer information; and even the California Data Privacy Law (California SB 1386), established to protect the confidential information of state residents.

Source: Computerworld

# Avoiding Spyware

---

By following certain steps, organizations and end users can reduce the risk of introducing spyware into the company. These measures include the following:

- Use antivirus software that identifies spyware.
- Download and execute code only from trusted sites.
- Update information security policies, if necessary, to include spyware. If file-sharing software is allowed, establish procedures for ensuring that it's configured correctly. If personal Internet use is allowed, establish criteria for appropriate use.
- Use discretion when clicking through online advertisements; ads that appear in a program's user interface are probably spyware.
- Review and revise firewall policies, if necessary, to ensure that only authorized outbound traffic is allowed. It may be necessary to install desktop firewalls to make sure spyware is blocked as it attempts to phone home.
- Become familiar with spyware sources and create rules to block access.



# Personal Spyware Tools

---

- Spybot ([www.majorgeeks.com](http://www.majorgeeks.com))
- Ad-aware ([www.majorgeeks.com](http://www.majorgeeks.com))
- Symantec Client Security
  - Personal Firewall
  - Personal Intrusion Detection
  - Antivirus



# What are we doing at MCG to protect you and your identity?

---

- Firewalls
- Network Intrusion Detection Systems
- Symantec Client Security
- Enterprise Server Manager
- User education
- Windows Updates Server
- Z.E.N. Works
- Plans to migrate away from SSN need
- Improved user account management.

# Sources

---

- Various web sites:
  - [www.identitytheft.org](http://www.identitytheft.org)
  - [www.idtheftcenter.org/](http://www.idtheftcenter.org/)
  - [www.techtv.com](http://www.techtv.com)
  - <http://www.epic.org/> (electronic privacy information center)
- Scene of the CyberCrime – Computer Forensics Handbook (Debra Littlejohn Shinder, Shingress Shinder Books)
- Security Alert: Stories of Real People Protecting Themselves from Identity Theft, Scams, and Viruses (Becky Worley, TechTV Books)



Questions?

---