PLUG IT IN 7

Protecting Your Information Assets

1. How to Protect Your Assets: The Basics
2. Behavioral Actions to Protect Your Information Assets
3. Computer-Based Actions to Protect Your Information Assets

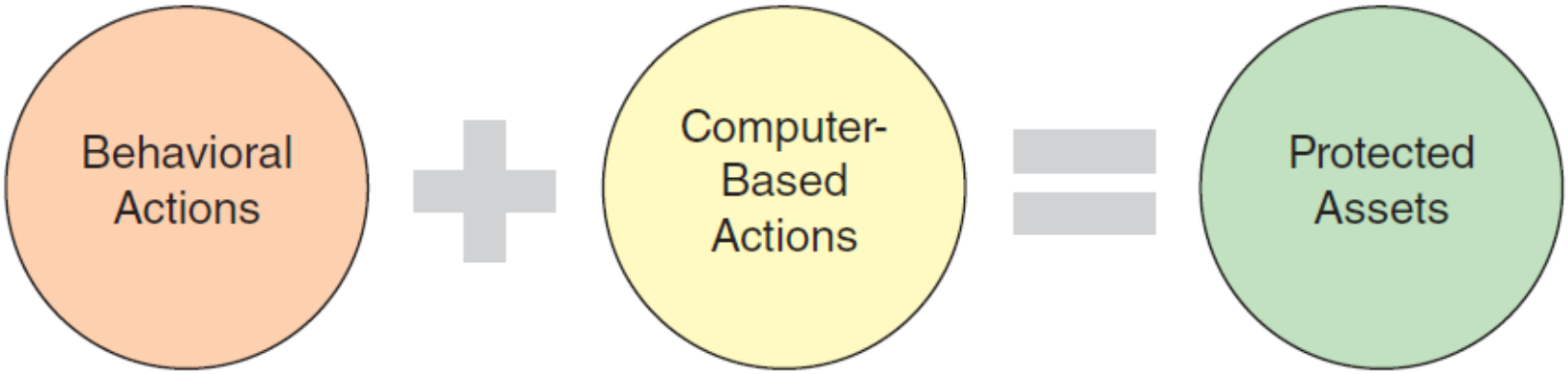
>>>

1. Explain why it is critical that you protect your information assets.
2. Identify the various behavioral actions you can take to protect your information assets.
3. Identify the various computer-based actions you can take to protect your information assets.

PI7.1 How to Protect Your Assets: The Basics

- Business travel
- Working from home
- Various activities at our favorite hotspot
- Industrial strength IS security from work
- Attacks on a home network

How to Protect Your Assets: The Basics



PI7.2 Behavioral Actions to Protect Your Information Assets

- General Behavioral Actions
- What to Do in the Event of Identity Theft

General Behavioral Actions

- Never provide personal information to anyone in any format
- Protect your Social Security number
- Use credit cards with your picture on them
- Write “Photo ID Required” on the back of credit cards

General Behavioral Actions (Continued)

- Use virtual credit cards
- Pay very close attention to your credit card billing cycles
- Receive your credit card bills electronically
- Only use the last four digits of your credit card account when paying by check

General Behavioral Actions (Continued)

- Limit your use of debit cards
- Use secure, private mailbox/PO Box
- Use a cross-cut or confetti shredder to dispose of old mail & records
- Sign up for a proactive protection service (e.g., lifelock.com, trustedid.com, cardcops.com)

What to Do in the Event of Identity Theft

- Review instructions from the Federal Trade Commission (FTC) and immediately take the actions outlined in the following slides.

What to Do in the Event of Identity Theft (continued)

Step 1:

- Place an Initial Fraud Alert by contacting all three credit reporting agencies (Equifax, Experian, Transunion
- Keep a detailed record of all communication (phone calls, letters, e-mail)

What to Do in the Event of Identity Theft (continued)

Step 2:

- Order credit reports from all three nationwide credit reporting companies.
- Keep detailed records of everything you requested and received

What to Do in the Event of Identity Theft (continued)

Step 3:

- Create and Identity Theft Report that includes an Identity Theft Affidavit and a police report.

What to Do in the Event of Identity Theft (continued)

Step 4:

- Regularly review your credit report.
- Pay particular attention to medical benefit explanations from your insurance company.
- Respond quickly to notices from the Internal Revenue Service (IRS)
- Obtain legal counsel

PI7.3 Computer-Based Actions to Protect Your Information Assets

- Determining Where People Have Visited on the Internet Using Your Computer
- The Dangers of Social Networking Sites
- Determining if Your Computer is Infected

PI7.3 Computer-Based Actions to Protect Your Information Assets (Continued)

- Computer Actions to Prevent Malware Infections
- Protecting Your Portable Devices and Information
- Other Actions You Can Take On Your Computer
- Protecting Your Privacy

PI7.3 Computer-Based Actions to Protect Your Information Assets (Continued)

- Preparing for Personal Disasters
- Wireless Security
- Mobile Security

Determining Where People Have Visited on the Internet Using Your Computer

Other people who may use your home computer may not practice "Safe Computing" practices

- Review the browser history
- Require a password for users on your home computer

The Dangers of Social Networking Sites

- Never post personal information about yourself or your family
- Deleted photos, posts, and messages can be copied and reposted by others
- Use the “Privacy Settings” to maintain control over your information

The Dangers of Social Networks

(Source: Jure Porenta / Shutterstock)

Determining if Your Computer is Infected

Signs that your computer system is infected with malicious software or malware

- Your computer shuts down unexpectedly by itself
- Your computer does not start normally

Determining if Your Computer is Infected (continued)

- Your computer exhibits erratic behavior, displaying some or all of these characteristics:
  - System runs out of hard drive space (memory)
  - System continually runs out of main memory (RAM)
  - Programs take longer to load than normal
  - Programs act erratically
  - Monitor displays strange graphics or messages.
  - System displays a high number of error messages.
  - Your e-mail client automatically sends messages to all your contacts

Computer Actions to Prevent Malware Infections

- Test Your System
- Install a Security Suite on Your Computer
- Install an Anti-malware Product on Your Computer
- Install a Firewall on Your Computer

Computer Actions to Prevent Malware Infections (con't)

- Install an Antispyware Product on Your Computer
- Install Monitoring Software on Your Computer
- Install Content-Filtering Software on Your Computer

Computer Actions to Prevent Malware Infections (con't)

- Install Antispam Software on Your Computer
- Manage Software Patches
- Use a Browser Other Than Internet Explorer
- Use an Operating System Other Than Windows

Protecting Your Portable Devices and Information

- Keep portable devices in an inconspicuous container/carrier
- Do not leave portable devices unattended in plain view
- Use alarms
- Two-factor authentication
- Use data encryption on portable devices

Other Actions You Can Take On Your Computer

- How to detect a worm
- How to detect a Trojan Horse
- How to detect fake Web Sites

Protecting Your Privacy

- Use strong passwords
- How to adjust your privacy settings on your computer
- How to surf the Web anonymously
- How to e-mail anonymously
- Erasing your Google search history

Preparing for Personal Disasters

- Safe deposit box for important papers
- Fireproof safe at home for important documents
- Regularly backup key computer files
- Encrypt backup files
- Backup to cloud or external drives

Wireless Security

- Hide your Service Set Identifier (SSID)
- Use encryption
- Filter out media access control addresses
- Limit IP Addresses
- Sniff out intruders

Wireless Security (continued)

- Using a Public Hotspot
- Test your wireless network
- Wireless security software

Mobile Security

- Mobile best practices
  - Strong password
  - Encrypted backups
  - Autolock option
  - Limit location based services
  - Maintain software/hardware updates
  - Be cautious when downloading apps