Module 11

Security Methods

Objectives

1. 2.3 Secure a Workstation
2. 2.4 Disposal Methods
3. 2.5 Wireless Security
4. 2.6 Wired Security

WORKSTATION SECURITY

Security Policy

1. A formal document defining network, computer, and user security protocols for a system or organization:
   A. For systems:
      - Limitations on functions
      - Limitations on access by external systems and users

   B. For an organization:
      - Limitations on behavior of its members
      - Limitations on physical security
2. Questions to answer in writing a local security policy:
   A. What assets require protection?
   B. What are the possible threats?
   C. What should be done in the event of a security breach?
   D. What are the user responsibilities?
   E. Crime and punishment

Protecting Physical Equipment

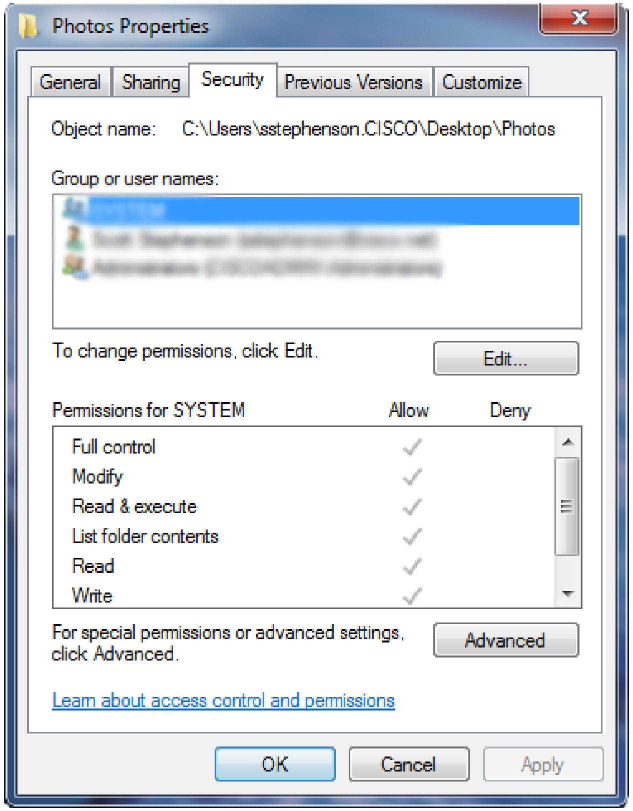
Since stealing the whole PC is the easiest way to steal data, physical computer equipment must be secured:

Physical Security Devices

1. Control access to facilities
2. Use cable locks
3. Lock telecommunication rooms
4. Use security screws
5. Use security cages around equipment
6. Label and install sensors on equipment

Protecting Digital Data

1. Methods of securing data:
   A. Password protection
   B. Restrict user permissions
   C. Disable guest accounts
   D. Screensaver passwords
   E. Data encryption
   F. Port protection
   G. Data backups
   H. File system security
   I. Disable autorun



Object name: C:\Users\sstephenson.CISCO\Desktop\Photos

Group or user names:

[redacted]

To change permissions, click Edit.

Permissions for SYSTEM	Allow	Deny
Full control	✓	
Modify	✓	
Read & execute	✓	
List folder contents	✓	
Read	✓	
Write	✓	

For special permissions or advanced settings, click Advanced.

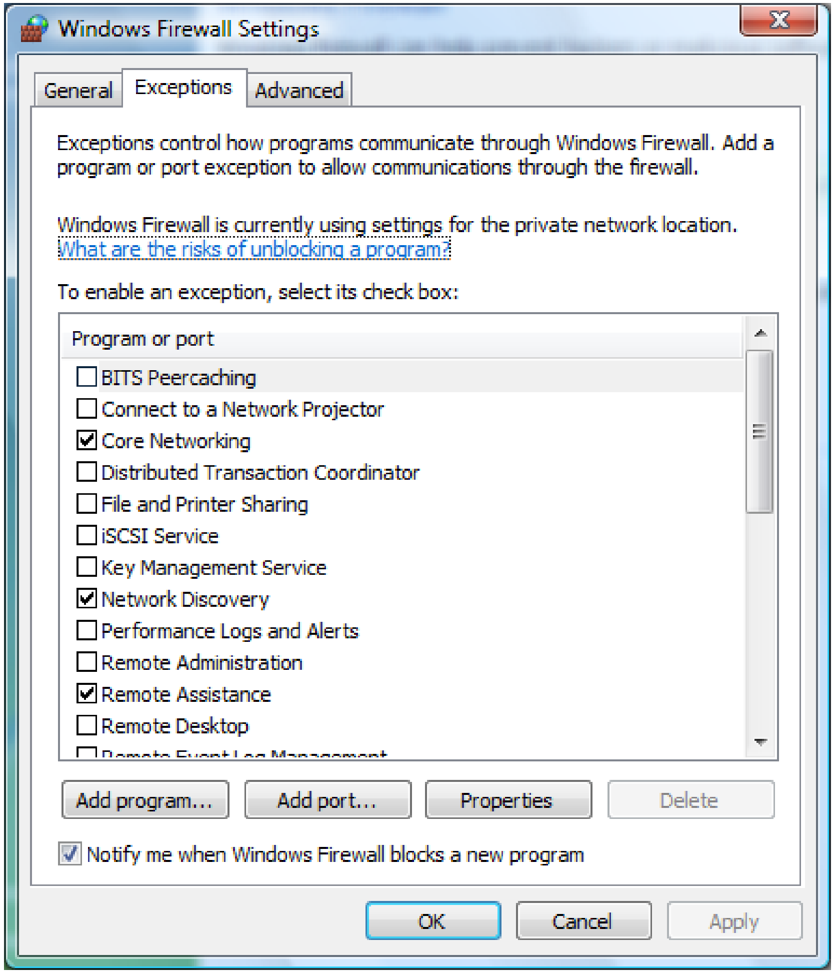
Learn about access control and permissions

Folder Security Properties

Personal Firewall

1. Firewall restricts what can come in and go out of your computer across the network:
   A. Stops bad stuff from coming in
   B. Stops a compromised computer from infecting other computers on network
2. **Two-way personal software firewall** – Inspects network traffic passing through it and denies/permits passage based on rules
3. **Application-aware firewall –** allows user to specify which desktop applications can connect to the network
4. A **Stateful Packet Inspection** (SPI):
   A. Tracks of the state of network connections
   B. Programmed to distinguish legitimate packets
   C. Only packets matching a known active connection will be allowed and all others will be rejected

Check Firewall Settings



Exceptions control how programs communicate through Windows Firewall. Add a program or port exception to allow communications through the firewall.

Windows Firewall is currently using settings for the private network location.
What are the risks of unblocking a program?

To enable an exception, select its check box:

Program or port

- □ BITS Peercaching
- □ Connect to a Network Projector
- ☑ Core Networking
- □ Distributed Transaction Coordinator
- □ File and Printer Sharing
- □ iSCSI Service
- □ Key Management Service
- ☑ Network Discovery
- □ Performance Logs and Alerts
- □ Remote Administration
- ☑ Remote Assistance
- □ Remote Desktop
- □ Remote Event Log Management

☑ Notify me when Windows Firewall blocks a new program

Update and Patch Management

Different types of Microsoft updates/patches:

1. **Important updates** – offer significant benefits, such as improved security, privacy, and reliability. They should be installed as they become available, and can be installed automatically with Windows Update.
2. **Recommended updates** – address non-critical problems or help enhance your computing experience. They should be installed as they become available, and can be installed automatically with Windows Update.
3. **Optional updates** – can include program updates, drivers, or new software from Microsoft to enhance your computing experience. You can only install these manually.

Patch Management

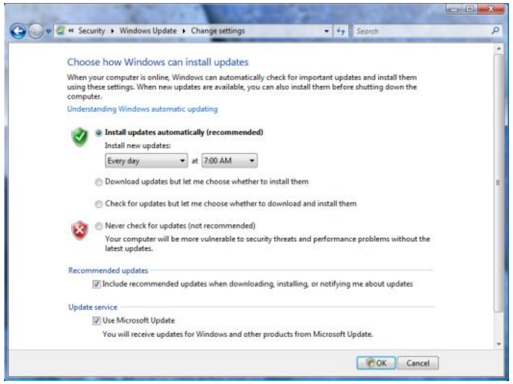
1. Depending on the type of update, Windows Update can deliver the following:

   A. **Security updates** – A broadly released fix for a product-specific security-related vulnerability. Security vulnerabilities are rated based on their severity, which is indicated in the Microsoft security bulletin as critical, important, moderate, or low

   B. **Critical updates** – A broadly released fix for a specific problem addressing a critical, non-security related bug

   C. **Service Packs** – A tested, cumulative set of hotfixes, security updates, critical updates, and important updates, as well as additional fixes for problems found internally since the release of the product. Service Packs might also contain customer requested design changes or features

2. How to install patch
3. Auto-update feature



Choose how Windows can install updates

When your computer is online, Windows can automatically check for important updates and install them using these settings. When new updates are available, you can also install them before shutting down the computer.

Understanding Windows automatic updating

● **Install updates automatically (recommended)**

Install new updates: Every day at 7:00 AM

○ Download updates but let me choose whether to install them

○ Check for updates but let me choose whether to download and install them

○ Never check for updates (not recommended)

Your computer will be more vulnerable to security threats and performance problems without the latest updates.

Recommended updates

☑ Include recommended updates when downloading, installing, or notifying me about updates

Update service

☑ Use Microsoft Update

You will receive updates for Windows and other products from Microsoft Update.

Automatic Updates Window

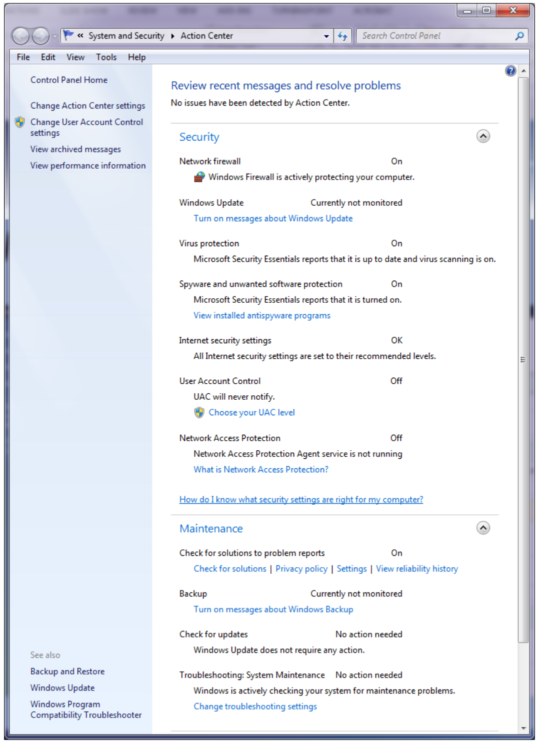
Know Your Antivirus/Antimalware

1. Know how to update
2. Know how to scan device
3. Know how to test antivirus
4. Know how to disinfect

Note: You should not install more than one antivirus program on a computer or they will conflict with each other. Then none of them will catch vulnerabilities.

Windows Action Center

1. Displays system security and maintenance features
2. Constantly monitors & displays the status of Windows Firewall, Automatic Updates, anti-virus, anti-spyware, Internet Explorer security settings, and User Account Control
3. First in Windows XP SP2
4. Vista name it Windows Security Center (WSC)
5. Windows 7 renamed to “Action Center”


« System and Security ▸ Action Center
Search Control Panel
File
Edit
View
Tools
Help
Control Panel Home
Change Action Center settings
Change User Account Control settings
View archived messages
View performance information
See also
Backup and Restore
Windows Update
Windows Program Compatibility Troubleshooter

Review recent messages and resolve problems

No issues have been detected by Action Center.

Security

Network firewall — On
Windows Firewall is actively protecting your computer.

Windows Update — Currently not monitored
Turn on messages about Windows Update

Virus protection — On
Microsoft Security Essentials reports that it is up to date and virus scanning is on.

Spyware and unwanted software protection — On
Microsoft Security Essentials reports that it is turned on.
View installed antispyware programs

Internet security settings — OK
All Internet security settings are set to their recommended levels.

User Account Control — Off
UAC will never notify.
Choose your UAC level

Network Access Protection — Off
Network Access Protection Agent service is not running
What is Network Access Protection?

How do I know what security settings are right for my computer?

Maintenance

Check for solutions to problem reports — On
Check for solutions | Privacy policy | Settings | View reliability history

Backup — Currently not monitored
Turn on messages about Windows Backup

Check for updates — No action needed
Windows Update does not require any action.

Troubleshooting: System Maintenance — No action needed
Windows is actively checking your system for maintenance problems.
Change troubleshooting settings

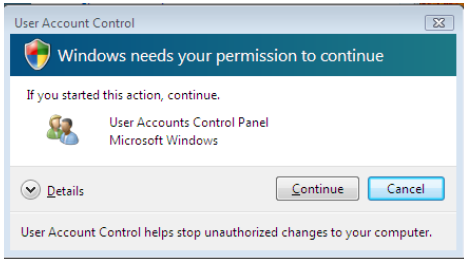
Action Center Window

User Account Control (UAC)

1. Alerts users of attempts to perform tasks that require administrative access then prompts for approval or an administrator password (if standard user)
2. Displays authentication dialog box that must be answered before continuing

   A. Administrators - Click Continue or Cancel

   B. Standard users - Enter admin password



User Account Control

Windows needs your permission to continue

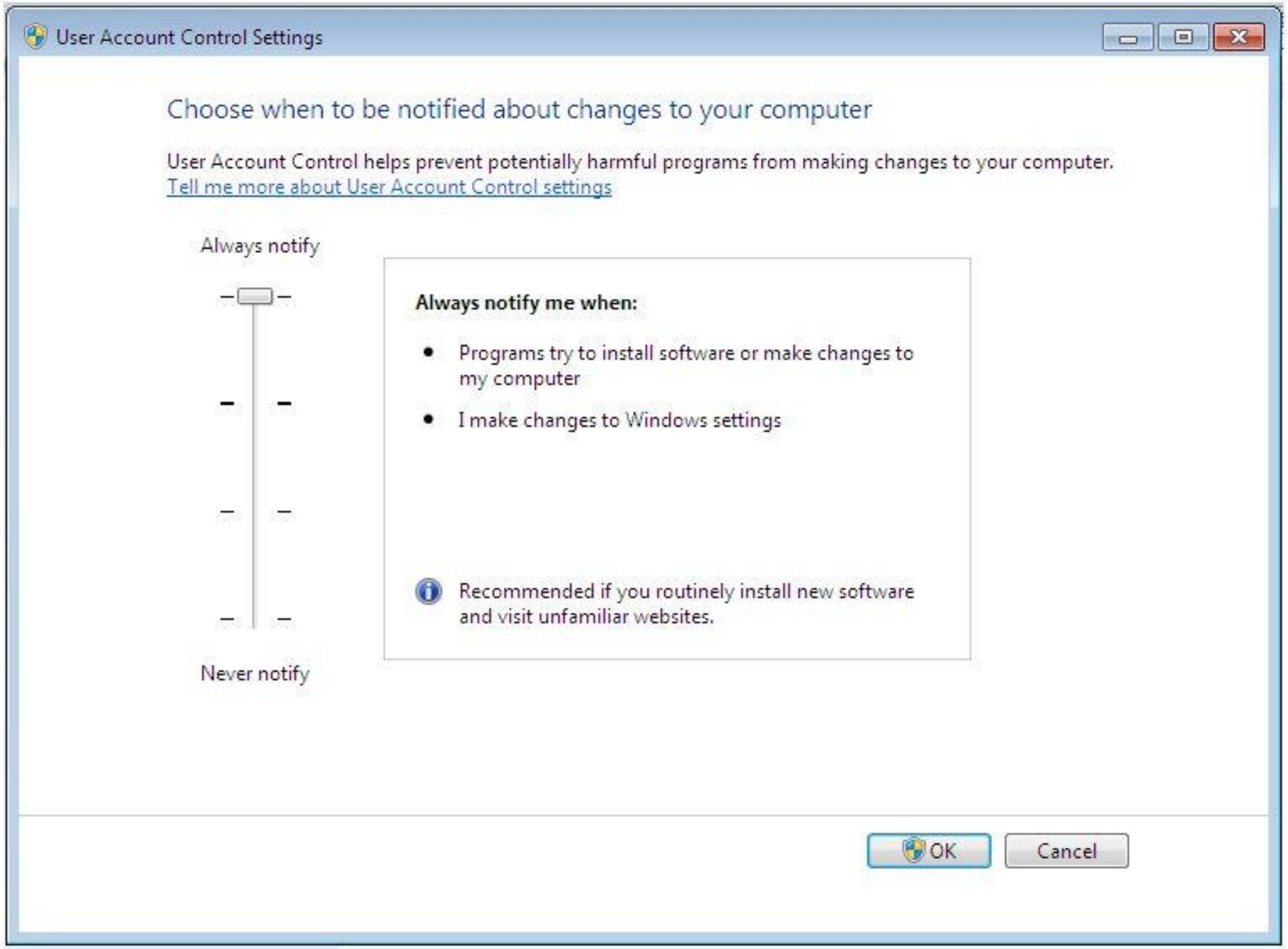
If you started this action, continue.

User Accounts Control Panel
Microsoft Windows

User Account Control helps stop unauthorized changes to your computer.

User Account Control

User Account Control (UAC)



Choose when to be notified about changes to your computer

User Account Control helps prevent potentially harmful programs from making changes to your computer.
Tell me more about User Account Control settings

Always notify me when:

- Programs try to install software or make changes to my computer
- I make changes to Windows settings

Recommended if you routinely install new software and visit unfamiliar websites.

DISPOSAL METHODS

Computer Disposal and Recycling

1. Data saved to a hard drive is persistent
2. Deleting data does not erase the data just the index
3. Remains on the drive until it is overwritten
4. To permanently get rid of data you can:
   A. Overwrite – Uses a special third-party software tools to repeatedly overwrite the data on a computer's hard drive with random 1s and 0s
   B. Secure erase – is a set of commands embedded on some hard drive that writes over every track on the drive but is disable by most BIOSs.
   C. Beginning in Windows Vista, a basic hard drive wipe is performed during a standard (non-quick) format

Computer Disposal and Recycling

5. Physical Destruction Methods:
   - A. To destroy software media (floppy disks and CDs), use a shredding machine designed for shredding these materials
   - B. Use an electromagnetic device or degaussing tool on the disk to scramble the bits
   - C. The only way to fully ensure that data cannot be recovered from a drive is to shatter the platters

INTERNET SECURITY

Internet Attacks

1. Attackers may use any of these tools to install a program on a computer:
   A. ActiveX
      - Controls interactivity on web pages
   B. Java
      - Allows applets to run within a browser
      - Example: a calculator or a calendar
   C. JavaScript
      - Interacts with HTML source code to allow interactive web sites
      - Example: a rotating banner or a popup window

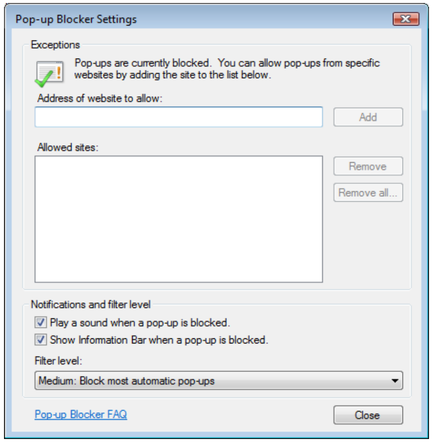
Spying Through Webcam

Internet Attacks

1. Privacy attacks
   A. Cookies
   B. Adware
2. Attacks while surfing
   A. Redirected Web traffic
   B. Drive-by downloads
3. E-mail attacks
   A. Spam
   B. Malicious attachments
   C. Embedded hyperlinks

Internet Defenses

1. Defenses through browser settings
   A. Advanced security settings
   B. Security zones
   C. Restricting cookies
   D. Popup blockers
2. Defenses through email applications
   A. Spam filters
   B. E-mail security settings
3. E-mail defenses through good practices



Pop-up Blocker Settings

Exceptions

Pop-ups are currently blocked. You can allow pop-ups from specific websites by adding the site to the list below.

Address of website to allow:

Allowed sites:

Notifications and filter level

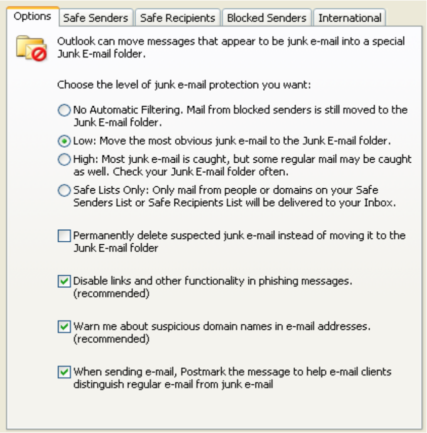
☑ Play a sound when a pop-up is blocked.

☑ Show Information Bar when a pop-up is blocked.

Filter level:

Medium: Block most automatic pop-ups

Popup Blocker



Outlook can move messages that appear to be junk e-mail into a special Junk E-mail folder.

Choose the level of junk e-mail protection you want:

○ No Automatic Filtering. Mail from blocked senders is still moved to the Junk E-mail folder.

● Low: Move the most obvious junk e-mail to the Junk E-mail folder.

○ High: Most junk e-mail is caught, but some regular mail may be caught as well. Check your Junk E-mail folder often.

○ Safe Lists Only: Only mail from people or domains on your Safe Senders List or Safe Recipients List will be delivered to your Inbox.

□ Permanently delete suspected junk e-mail instead of moving it to the Junk E-mail folder

☑ Disable links and other functionality in phishing messages. (recommended)

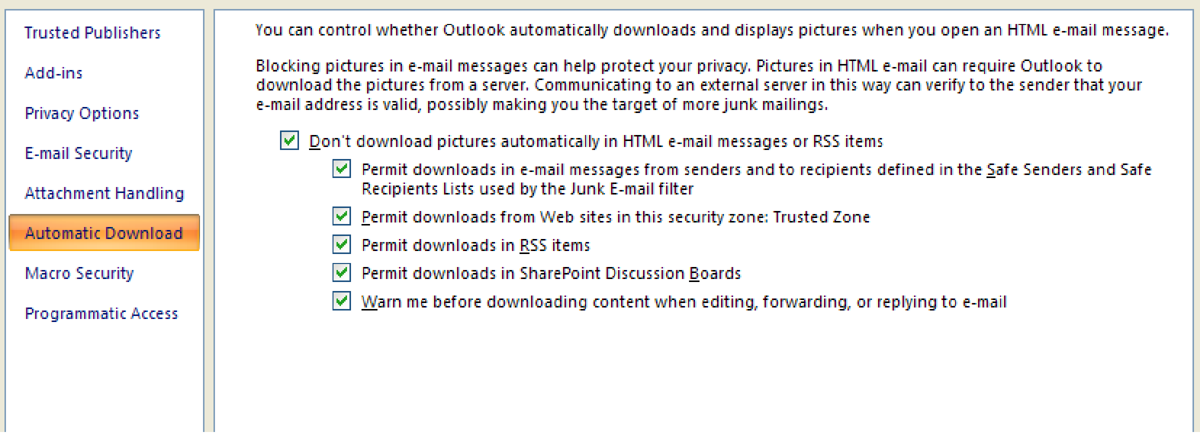
☑ Warn me about suspicious domain names in e-mail addresses. (recommended)

☑ When sending e-mail, Postmark the message to help e-mail clients distinguish regular e-mail from junk e-mail

Email Spam Filter

E-Mail Security Settings

1. Read messages using a reading pane
2. Preview attachments
3. Block external content



You can control whether Outlook automatically downloads and displays pictures when you open an HTML e-mail message.

Blocking pictures in e-mail messages can help protect your privacy. Pictures in HTML e-mail can require Outlook to download the pictures from a server. Communicating to an external server in this way can verify to the sender that your e-mail address is valid, possibly making you the target of more junk mailings.

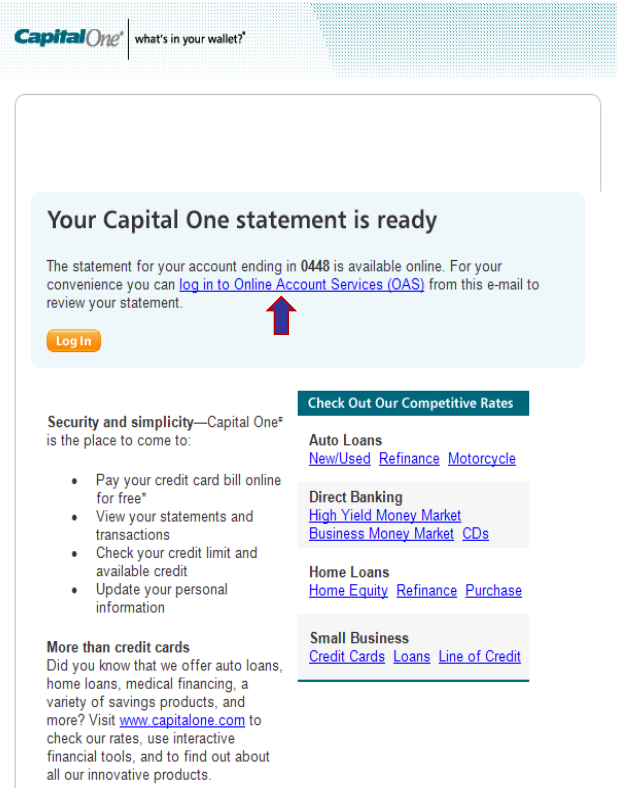
- ☑ Don't download pictures automatically in HTML e-mail messages or RSS items
  - ☑ Permit downloads in e-mail messages from senders and to recipients defined in the Safe Senders and Safe Recipients Lists used by the Junk E-mail filter
  - ☑ Permit downloads from Web sites in this security zone: Trusted Zone
  - ☑ Permit downloads in RSS items
  - ☑ Permit downloads in SharePoint Discussion Boards
  - ☑ Warn me before downloading content when editing, forwarding, or replying to e-mail

Email Security Settings

Embedded Hyperlink

1. . . . you can <a href="http://www.capitalone.com">log in to Online Account Services (OAS) </a> from this e-mail

2. . . . you can <a href="http://www.steal-your-number.net">log in to Online Account Services (OAS) </a> from this e-mail



Your Capital One statement is ready

The statement for your account ending in **0448** is available online. For your convenience you can log in to Online Account Services (OAS) from this e-mail to review your statement.

Security and simplicity—Capital One® is the place to come to:

- Pay your credit card bill online for free*
- View your statements and transactions
- Check your credit limit and available credit
- Update your personal information

More than credit cards
Did you know that we offer auto loans, home loans, medical financing, a variety of savings products, and more? Visit www.capitalone.com to check our rates, use interactive financial tools, and to find out about all our innovative products.

Check Out Our Competitive Rates

Auto Loans
New/Used Refinance Motorcycle

Direct Banking
High Yield Money Market
Business Money Market CDs

Home Loans
Home Equity Refinance Purchase

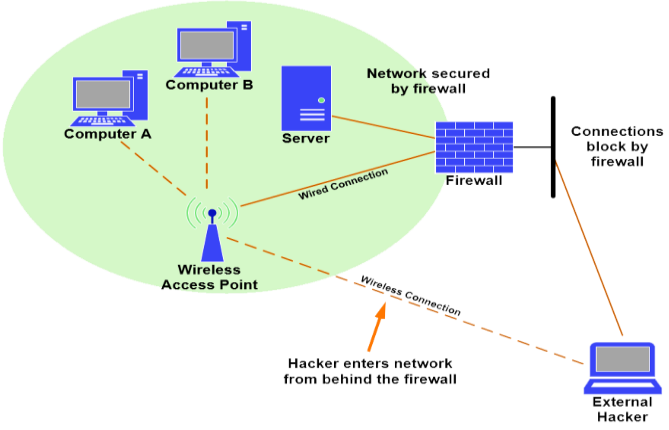
Small Business
Credit Cards Loans Line of Credit

Fake Email

WIRELESS SECURITY

Does Wireless Security Matter?

1. Get into any folder set with file sharing enabled
2. See wireless transmissions
3. Access network behind firewall can inject malware
4. Download harmful content linked to unsuspecting owner



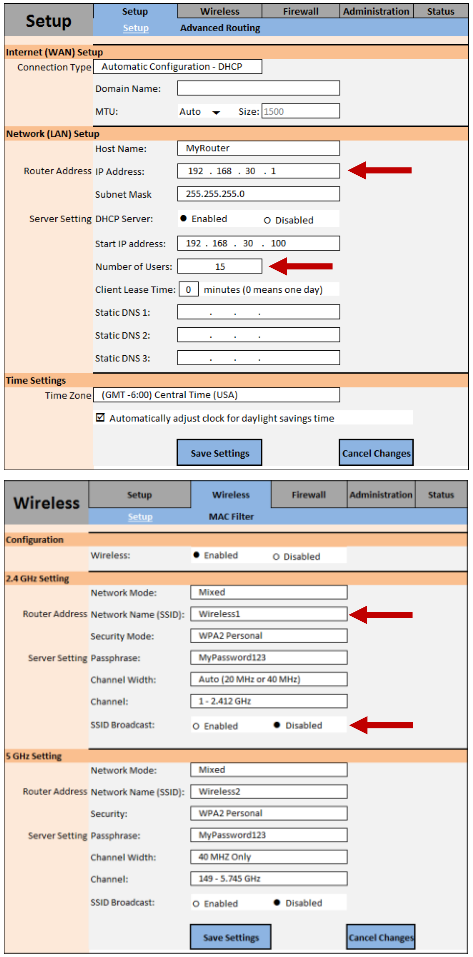
Typical Network Behind Firewall

1. Lock Down AP

1. Change the default password and create a strong Password
2. Disable Wireless Web Access (cannot access AP settings via wireless device, must be connected with cable)
3. Disable Remote Management (cannot access AP settings via Internet)
4. Access server via HTTPS
5. Disable UPnP

2. Access

1. Change the default IP address
2. Limit DHCP addresses
3. Change the default SSID
4. Disable SSID broadcast



Internet (WAN) Setup

Connection Type: Automatic Configuration - DHCP

Domain Name:

MTU: Auto Size: 1500

Network (LAN) Setup

Host Name: MyRouter

Router Address IP Address: 192 . 168 . 30 . 1

Subnet Mask 255.255.255.0

Server Setting DHCP Server: ● Enabled ○ Disabled

Start IP address: 192 . 168 . 30 . 100

Number of Users: 15

Client Lease Time: 0 minutes (0 means one day)

Static DNS 1: . . .

Static DNS 2: . . .

Static DNS 3: . . .

Time Settings

Time Zone: (GMT -6:00) Central Time (USA)

☑ Automatically adjust clock for daylight savings time

Configuration

Wireless: ● Enabled ○ Disabled

2.4 GHz Setting

Network Mode: Mixed

Router Address Network Name (SSID): Wireless1

Security Mode: WPA2 Personal

Server Setting Passphrase: MyPassword123

Channel Width: Auto (20 MHz or 40 MHz)

Channel: 1 - 2.412 GHz

SSID Broadcast: ○ Enabled ● Disabled

5 GHz Setting

Network Mode: Mixed

Router Address Network Name (SSID): Wireless2

Security: WPA2 Personal

Server Setting Passphrase: MyPassword123

Channel Width: 40 MHZ Only

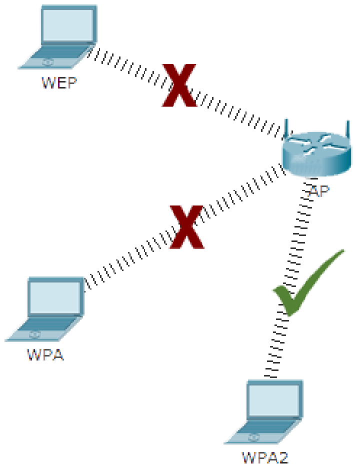
Channel: 149 - 5.745 GHz

SSID Broadcast: ○ Enabled ● Disabled

Wireless Access Point

Levels of Wireless Security

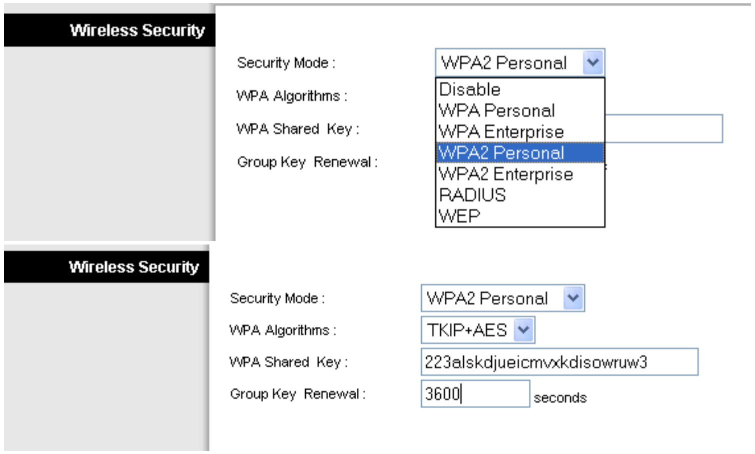
1. **Wired Equivalent Privacy** (WEP) is an outdated wireless security that uses either 64- or 128-bit encryption
2. **Wi-Fi Protected Access** (WPA or WPA2) uses 128- or 256-bit encryption
   - A. **Personal** is managed by the router and uses the Shared Key
   - B. **Enterprise** is intended for businesses using a Radius server to authenticate users



Wireless Security

3. Turn on WPA2

1. On AP Security Mode set as WPA2 Personal
2. WPA Algorithms set as TKIP+AES (AES is best)
3. WPA Shared Key set minimum 8 characters
4. Group Key Renewal should not be set to less than 300 seconds (5 minutes)



Security Mode : WPA2 Personal

WPA Algorithms :

WPA Shared Key :

Group Key Renewal :

Wireless Security

Security Mode : WPA2 Personal

WPA Algorithms : TKIP+AES

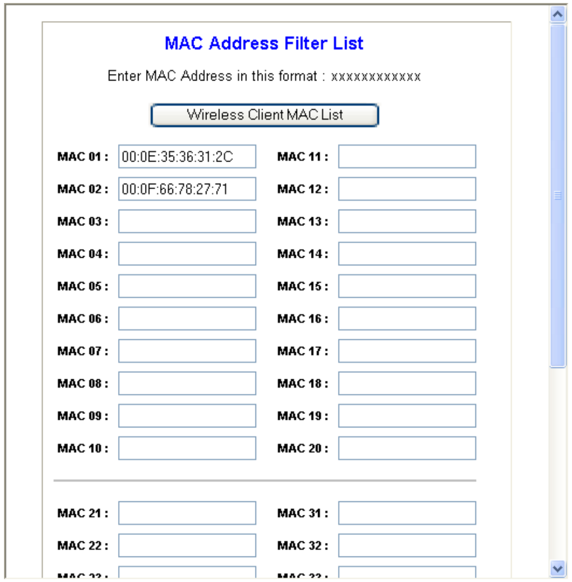
WPA Shared Key : 223alskdjueicmvxkdisowruw3

Group Key Renewal : 3600 seconds

Wireless Security

4. Limit Users By MAC

1. Edit MAC Filter List by entering MAC addresses of approved PCs
2. Permit only PCs listed to access the wireless network
3. Enable Wireless MAC Filter
4. Be sure to “Edit”, “Permit” then “Enable” or else cannot let yourself in



MAC Address Filter List

Enter MAC Address in this format : xxxxxxxxxxxx

MAC 01 :	00:0E:35:36:31:2C	MAC 11 :	
MAC 02 :	00:0F:66:78:27:71	MAC 12 :	
MAC 03 :		MAC 13 :	
MAC 04 :		MAC 14 :	
MAC 05 :		MAC 15 :	
MAC 06 :		MAC 16 :	
MAC 07 :		MAC 17 :	
MAC 08 :		MAC 18 :	
MAC 09 :		MAC 19 :	
MAC 10 :		MAC 20 :	
MAC 21 :		MAC 31 :	
MAC 22 :		MAC 32 :	
MAC 23 :		MAC 33 :	

MAC Filtering

5. Apply after all devices have connected so they will appear in the list

Summary

In this module we discussed:

1. Security Policies
2. Physical and Digital Security
3. Firewalls
4. Updates and Patches
5. Windows Action Center
6. User Account Controls
7. Disposal Methods
8. Types on Internet attacks
9. Wireless Security

Glossary and Terms

1. **Security Policy** - A formal document defining network, computer, and user security protocols for a system or organization.
2. **Two-way personal software firewall** – Inspects network traffic passing through it and denies/permits passage based on rules
3. **Application-aware firewall – A**llows user to specify which desktop applications can connect to the network.
4. **SPI –** Stateful Packet Inspection**.** Tracks of the state of network connections and only packets matching a known active connection to enter and all others will be rejected
5. **Service Packs** – A tested, cumulative set of hotfixes, security updates, critical updates, and updates, as well as additional fixes for problems found internally since the release of the product. Service Packs might also contain customer requested design changes or features.

Glossary and Terms

6. **Windows Action Center** – Displays system security and maintenance features in Windows 7. Constantly monitors & displays the status of Windows Firewall, Automatic Updates, anti-virus, anti-spyware, Internet Explorer security settings, and User Account Control
7. **UAC** – User Account Control. Alerts users of attempts to perform tasks that require administrative access then prompts for approval or an administrator password (if standard user).
8. **ActiveX** – Microsoft application that controls interactivity on web pages.
9. **Java** – A program by Sun Microsystems that allows applets to run within a browser like a calculator or a calendar.

Glossary and Terms

10.**JavaScript** – Interacts with HTML source code to allow interactive web sites like a rotating banner or a popup window.

11.**Cookies** – A small piece of data sent to a website that contains information about the user. It is stored in the user's computer.

12.**Hyperlink** – Text that automatically points to a document or web page.

13.**HTTP** – HyperText Transfer Procotol

14.**HTTPS** – HyperText Transfer Procotol with Security

14.**UPnP** – Universal Plug-and-Play

15.**DHCP** – Dynamic Host Control Protocol

Glossary and Terms

16. **SSID** – Service Set Identifier
17. **WEP** – Wired Equivalent Privacy is an outdated wireless security that uses either 64- or 128-bit encryption.
18. **WPA** – Wi-Fi Protected Access is the current wireless security protocol that uses 128- or 256-bit encryption.
19. **TKIP** – Temporal Key Integrity Protocol
20. **AES** – Advanced Encryption Standard
21. **MAC** – Media Access Control