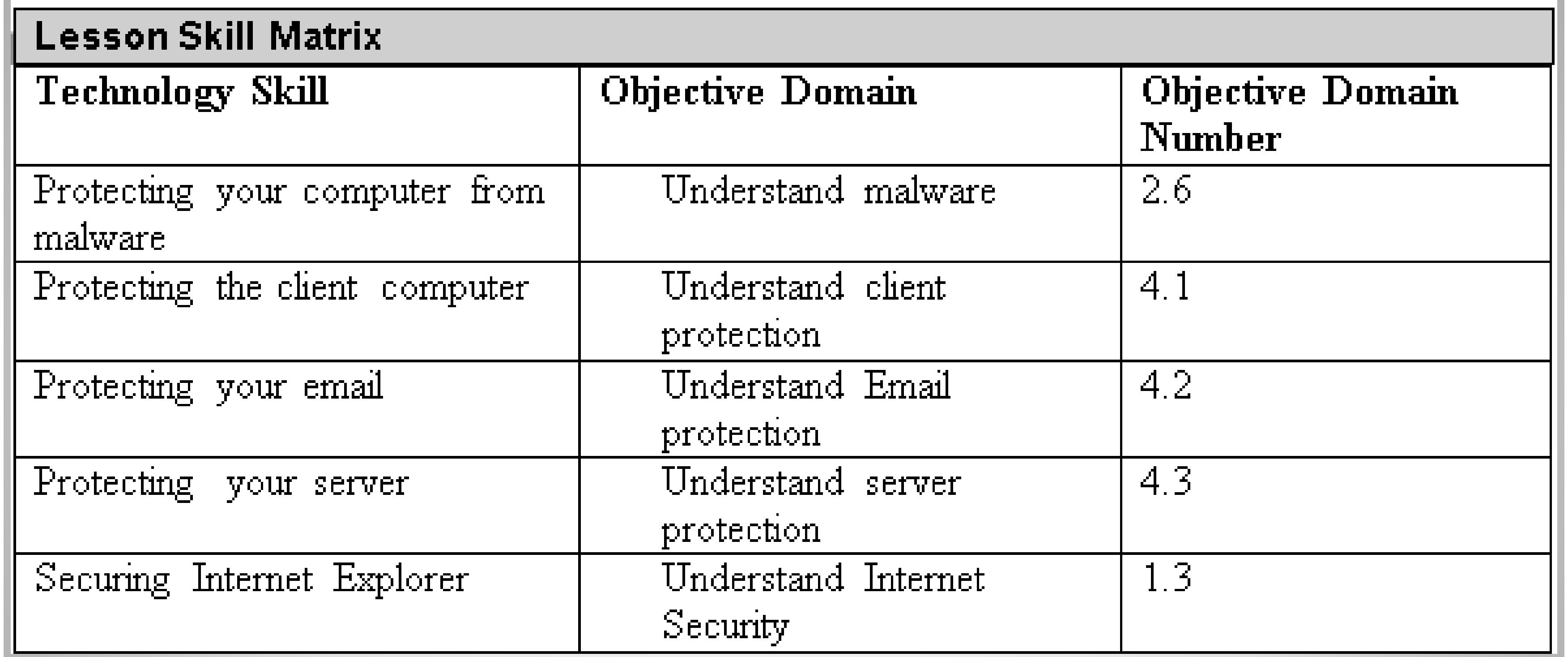
Protecting the Server and Client

Lesson 5

Objectives



Lesson Skill Matrix

Technology Skill	Objective Domain	Objective Domain Number
Protecting your computer from malware	Understand malware	2.6
Protecting the client computer	Understand client protection	4.1
Protecting your email	Understand Email protection	4.2
Protecting your server	Understand server protection	4.3
Securing Internet Explorer	Understand Internet Security	1.3

Malicious Software

- Malicious software, sometimes called malware, is software designed to infiltrate or affect a computer system without the owner’s informed consent.
- It is usually associated with virus, worms, Trojan horses, spyware, rootkits and dishonest adware.

Virus

- A computer ***virus*** is a program that can copy itself and infect a computer without the user’s consent or knowledge.
- Early viruses were usually some form of executable code that was hidden in the boot sector of a disk or as an executable file (filename with an .exe or .com filename extension).
- Later, as macros languages were used in software application such as word processors and spreadsheets to enhance the programs power and flexibility, macro programs can be embedded within the documents, which can cause harm.

Worm

- A worm is a self-replicating program that replicates itself to other computers over the network without any user intervention.
- Different from a virus, a worm does not corrupt or modify files on a target computer.
- Instead, it consumes bandwidth and as well as processor and memory resources, slowing your system down or causing your system to be unusable.
- Worms usually spread by using security holes found within the operating system or TCP/IP software implementations.

Trojan Horse and Spyware

- A Trojan horse is an executable program that appears as a desirable or useful program. Since it appears to be a desirable or useful program, user are tricked into loading and executing the program on their system.
- Spyware is a type of malware that is installed on computers and collects personal information or browsing habits often without the user’s knowledge.

Rootkit and Backdoor

- A rootkit is a software or hardware device designed to gain administrator-level control over a computer system without being detected.
- A backdoor is a program that gives some remote, unauthorized control of a system or initiates an unauthorized task.

Virus Symptoms

- Poor system performance
- Your system has less available memory than it should
- Poor performance while connected to the Internet.
- Computer stops responding frequently.
- Computer takes longer to start up.
- Browser closes unexpected or stop responding.
- Default home or default search pages change in your browser.
- Unexpected Pop-up advertising windows.
- Unexpected additional toolbars added to the browser.
- Unexpected programs automatically start.
- Cannot start a program.

Virus Symptoms

- Components of Windows or other programs no longer work.
- Programs or files are suddenly missing.
- Unusual messages or displays on your monitor.
- Unusual sounds or music played at random times.
- System has less available memory than it should.
- Unknown programs or files have been created installed.
- Your browser has unknown add-ins.
- Files have become corrupted.
- File size unexpectedly changes.

Protecting Against Malware

- The first step that you need to protect yourself against malware is to keep your system up-to-date with the latest service packs, security patches and other critical fixes.
- The second step to protect your computer from malware is to use an up-to-date antivirus software package.

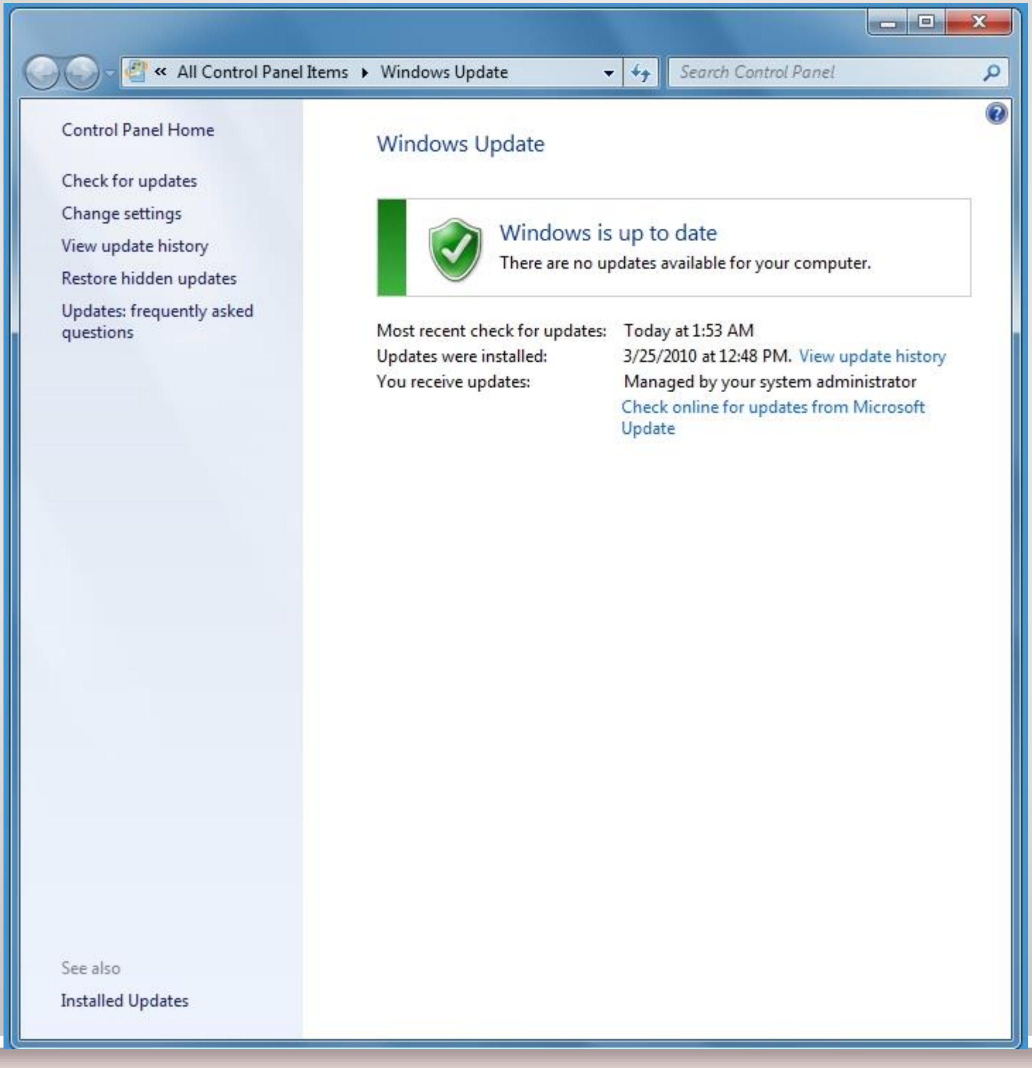
Virus Hoax

- A ***virus hoax*** is a message warning the recipient of non-existent computer virus threat, usually sent as a chain email that tells the recipient to forward it to everyone they know.
- This is a form of social engineering that plays on people’s ignorance and fear.

Windows Updates

- After installing Windows, check to see if Microsoft has any ***Windows updates*** including fixes, patches, service packs and updated device drivers, and apply them to the Windows system.
- By adding fixes and patches, you will keep Windows stable and secure.
- If there are many fixes or patches, Microsoft releases them together as a service pack or a cumulative package.

Windows Updates



Windows Update

Windows is up to date

There are no updates available for your computer.

Most recent check for updates: Today at 1:53 AM

Updates were installed: 3/25/2010 at 12:48 PM. View update history

You receive updates: Managed by your system administrator

Check online for updates from Microsoft Update

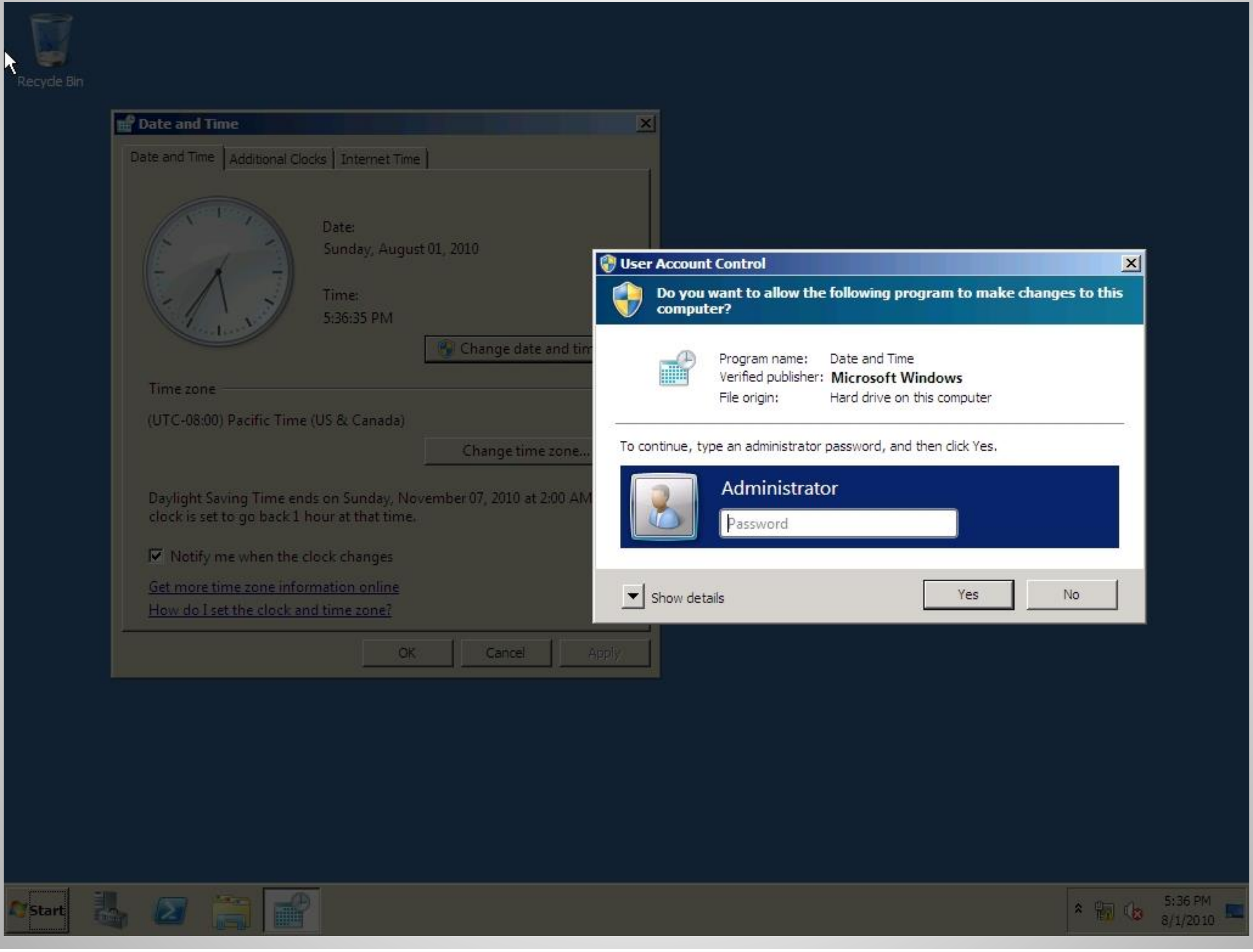
WSUS and SCCM

- For corporations, you can also use ***Windows Server Update Service (WSUS)*** or System Center Configuration Manager (SCCM) to keep your systems updates.
- The advantages of using one of these two systems allow you to test the patch, schedule the updates and prioritize client updates.
- When you consider the patch is safe to deploy, you then enable the patch for deployment.

User Account Control (UAC)

- ***User Account Control (UAC)*** is a feature that started with Windows Vista and is included with Windows 7 that helps prevent unauthorized changes to your computer.
- Therefore, UAC helps you protect your system from malware.

User Account Control (UAC)



Date:
Sunday, August 01, 2010

Time:
5:36:35 PM

Time zone

(UTC-08:00) Pacific Time (US & Canada)

Daylight Saving Time ends on Sunday, November 07, 2010 at 2:00 AM
clock is set to go back 1 hour at that time.

☑ Notify me when the clock changes

Get more time zone information online

How do I set the clock and time zone?

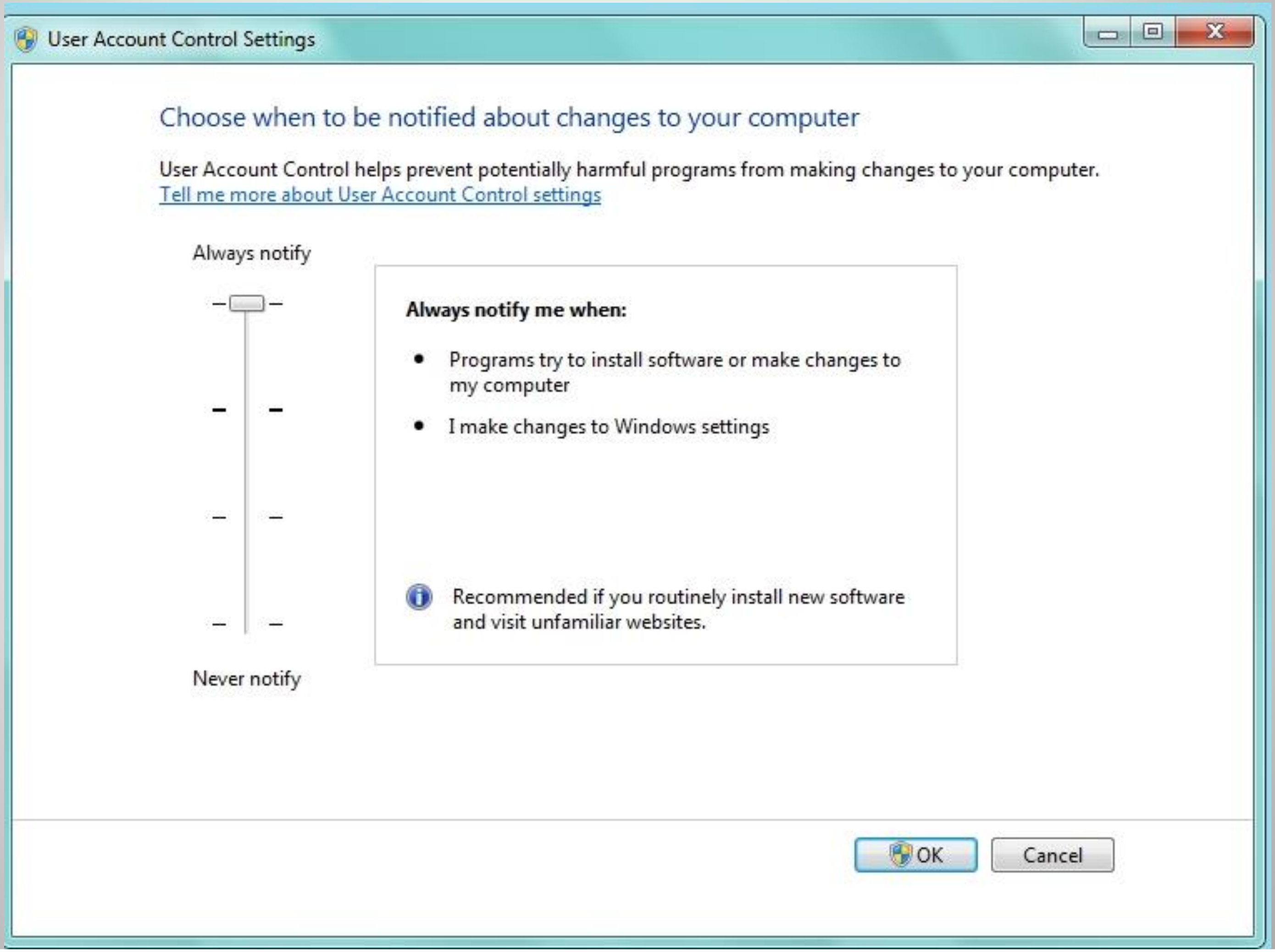
Do you want to allow the following program to make changes to this computer?

Program name: Date and Time
Verified publisher: **Microsoft Windows**
File origin: Hard drive on this computer

To continue, type an administrator password, and then click Yes.

Administrator
Password

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.

Windows Firewall

- A firewall can help prevent hackers or malicious software (such as worms) from gaining access to your computer through a network or the Internet.
- A firewall can also help stop your computer from sending malicious software to other computers.
- Microsoft recommends that you should always use the ***Windows Firewall***.

Offline Files

- ***Offline files*** are copies of network files that are stored on your computer so that you can access them when you are not connected to the network or when the network folder with the files is not connected.
- Offline files are not encrypted unless you choose to do so.
- You might want to encrypt your offline files if they contain sensitive or confidential information and you want to make them more secure by restricting access to them.

Protecting Email

- Email has become an essential service for virtually every corporation.
- Unfortunately, most email received will be unsolicited emails called ***spam*** or junk email, some of which can carry malware and may lead to fraud or scams.
- To keep your systems running smoothly, it is important for a network administrator put some effort into blocking spam.

Spam Filtering System

- Spam filtering systems will not catch every single spam message.
- But like an anti-virus package, the spam filtering solution needs to be kept up-to-date and needs to be constantly tweaked.
- Many anti-spam solutions will also use a Real-time Blackhole Lists (RBLs) or DNS-based Blackhole List (DNSBL) which can be accessed freely.

Sender Policy Framework (SPF)

- Sender Policy Framework (SPF) is an email validation system designed to prevent e-mail spam done with source address spoofing.
- SPF allows administrators to specify which hosts are allowed to send e-mail from a given domain as specified in a specific DNS SPF record in the public DNS.
- If email for a domain is not sent from a host listed in the DNS SPF, it will be considered spam and blocked.

SMTP Relay

- One of the primary email protocols is SMTP. Simple Mail Transfer Protocol (SMTP) is used to transfer email from one server to another and it is responsible for outgoing mail transport. SMTP uses TCP port 25.
- While you may think that your email servers are only used for your users to send and retrieve email, they are also used to relay email.
- Usually, you only want your internal servers to relay email through your mail servers.
- Unfortunately, spammers look for unprotected SMTP servers to relay their email through.

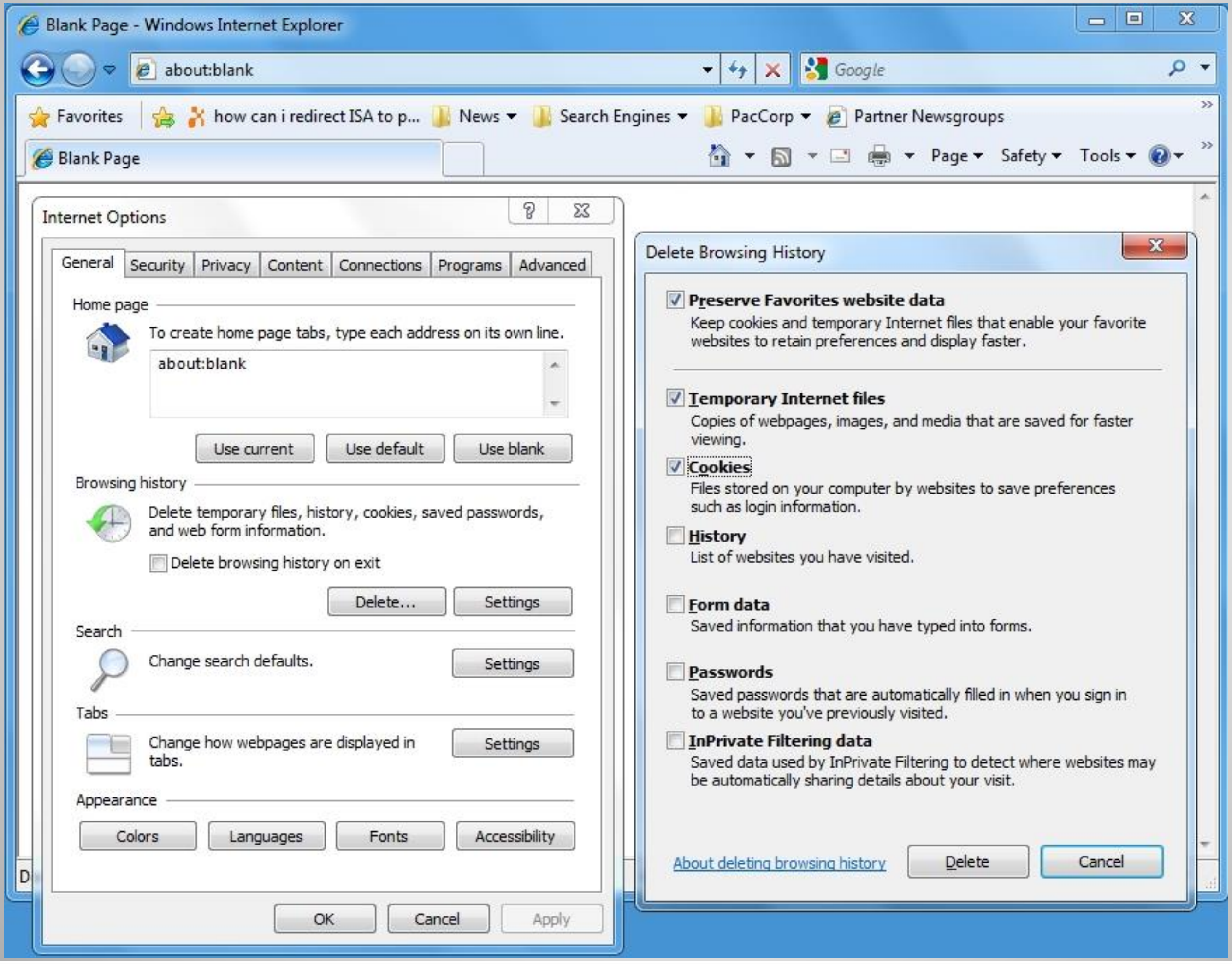
Browsing the Internet

- Since browsing a website can expose you to a wide range of hazards, you also need to look at your browser to help protect you and your system.
- Today’s browsers include pop-up blocker’s, the use of zones and other built-in security features.

Cookies and Privacy Settings

- When you use a browser to access the Internet, a lot can be revealed about a person's personality and personal information.
- Therefore, you need to take steps to ensure that this information cannot be read or used without your knowledge.
- A ***cookie*** is a piece of text stored by a user's web browser.
  - It can be used for a wide range of items including user identification, authentication, storing site preferences and shopping cart contents.

Deleting Cookies and Other Information



Internet Options

Home page

To create home page tabs, type each address on its own line.

about:blank

Browsing history

Delete temporary files, history, cookies, saved passwords, and web form information.

□ Delete browsing history on exit

Search

Change search defaults.

Tabs

Change how webpages are displayed in tabs.

Appearance

Delete Browsing History

☑ **Preserve Favorites website data**
Keep cookies and temporary Internet files that enable your favorite websites to retain preferences and display faster.

☑ **Temporary Internet files**
Copies of webpages, images, and media that are saved for faster viewing.

☑ **Cookies**
Files stored on your computer by websites to save preferences such as login information.

□ **History**
List of websites you have visited.

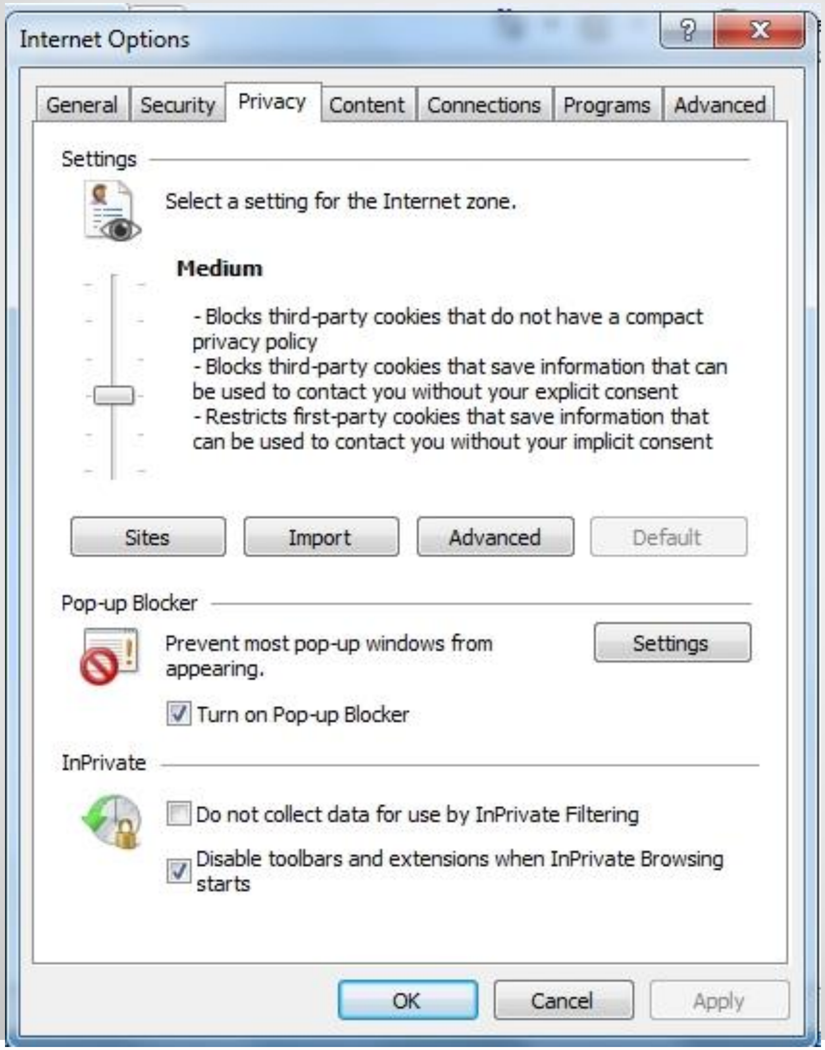
□ **Form data**
Saved information that you have typed into forms.

□ **Passwords**
Saved passwords that are automatically filled in when you sign in to a website you've previously visited.

□ **InPrivate Filtering data**
Saved data used by InPrivate Filtering to detect where websites may be automatically sharing details about your visit.

About deleting browsing history

IE Privacy Settings



Settings

Select a setting for the Internet zone.

Medium

- Blocks third-party cookies that do not have a compact privacy policy
- Blocks third-party cookies that save information that can be used to contact you without your explicit consent
- Restricts first-party cookies that save information that can be used to contact you without your implicit consent

Pop-up Blocker

Prevent most pop-up windows from appearing.

☑ Turn on Pop-up Blocker

InPrivate

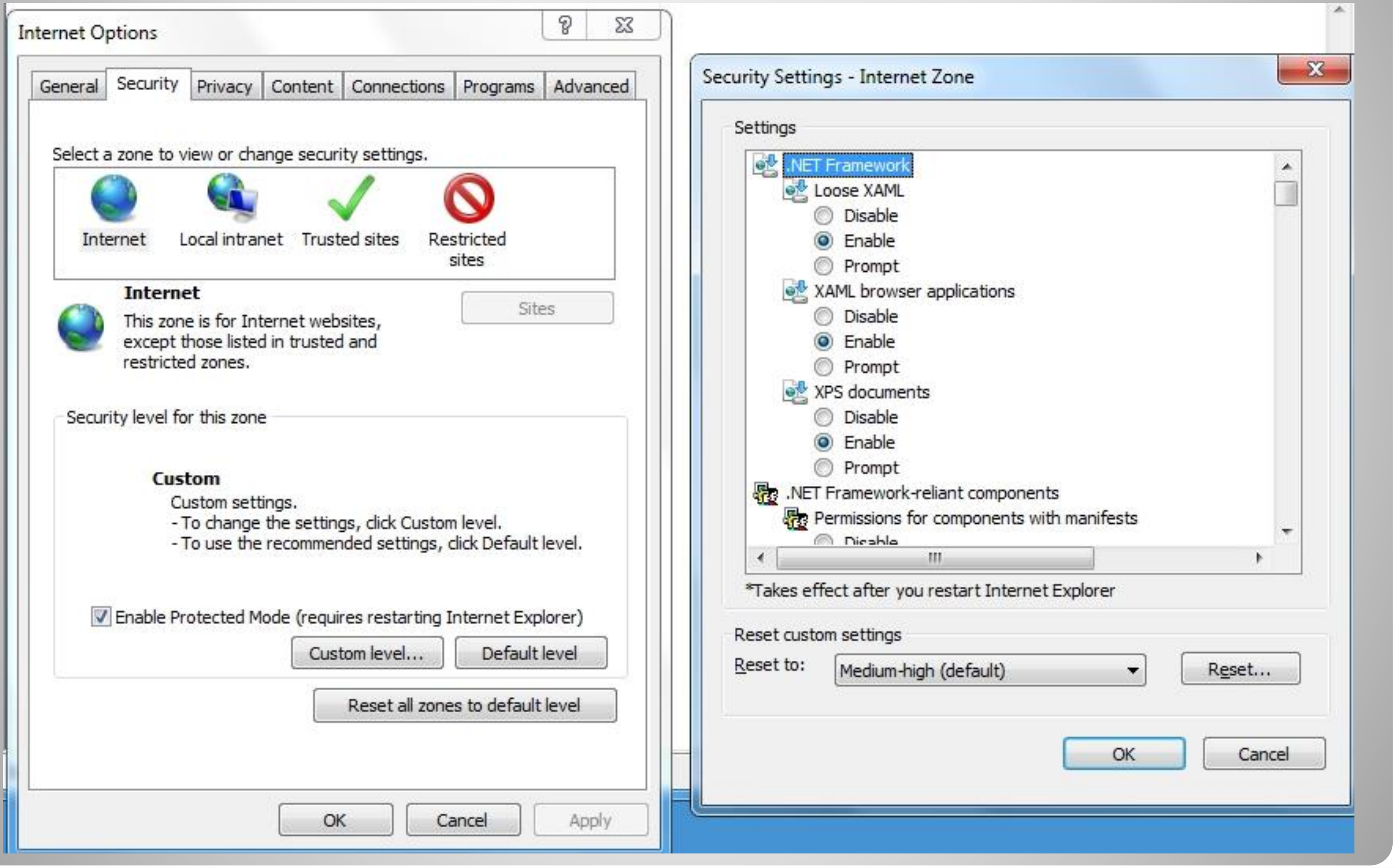
□ Do not collect data for use by InPrivate Filtering

☑ Disable toolbars and extensions when InPrivate Browsing starts

Content Zones

- To help manage Internet Explorer security when visiting sites, Internet Explorer divides your network connection into four content zones or types:
  - Internet Zone
  - Local Intranet Zone
  - Trusted Sites Zone
  - Restricted Sites Zone

Content Zones



Internet Options

Select a zone to view or change security settings.

Internet

This zone is for Internet websites, except those listed in trusted and restricted zones.

Security level for this zone

Custom

Custom settings.
- To change the settings, click Custom level.
- To use the recommended settings, click Default level.

☑ Enable Protected Mode (requires restarting Internet Explorer)

Security Settings - Internet Zone

Settings

- .NET Framework
  - Loose XAML
    - ○ Disable
    - ● Enable
    - ○ Prompt
  - XAML browser applications
    - ○ Disable
    - ● Enable
    - ○ Prompt
  - XPS documents
    - ○ Disable
    - ● Enable
    - ○ Prompt
- .NET Framework-reliant components
  - Permissions for components with manifests
    - ○ Disable

*Takes effect after you restart Internet Explorer

Reset custom settings

Reset to: Medium-high (default)

Phishing

- ***Phishing*** is a technique based on social engineering. With phishing, users are asked (usually through email or other websites) to supply personal information by:
  - Having an email asking your username, password and other personal information such as account numbers, PINs and social security numbers.
  - Redirect a user to a convincing-looking web site that urges users to supply personal information, such as passwords and account numbers.

Phishing

- To help protect against Phishing, Internet Explorer 8 includes SmartScreen Filter that examines traffic for evidence of phishing activity and displays a warning to the user if it finds any.

Pharming

- ***Pharming*** is an attack aimed at redirecting a website's traffic to bogus website.
- This is usually accomplished by changing the hosts file (a text that provides name resolution for host or domain names to IP address) on a computer or by exploiting a vulnerability on a DNS server.

SSL

- When you surf the Internet, there are times when you need to transmit private data over the Internet such as credit card numbers, social security numbers and so on.
- During these times, you should be using http over SSL (https) to encrypt the data sent over the Internet.
- By convention, URLs that require an SSL connection start with https: instead of http:.

Protecting your Server

- The first step in securing a server is where to place the server.
  - The server should be kept in a secure location.
  - In addition, the servers should be in their own subnet and VLAN to reduce the traffic to the servers including broadcasts.
- The next step in securing a server is to harden the server where you reduce the surface of attack and you reduce the server’s vulnerabilities.

Microsoft Baseline Security Analyzer (MBSA)

- Microsoft Baseline Security Analyzer (MBSA) is a software tool released by Microsoft to determine the security state of a system by assessing missing security updates and less-secure security settings within Microsoft Windows, Windows components such as Internet Explorer, IIS web server, and products Microsoft SQL Server, and Microsoft Office macro settings.

Secure Dynamic DNS

- Dynamic DNS lets client computers dynamically update their resource records in DNS.
- With typical unsecured dynamic updates, any computer can create records on your DNS server which leaves you open to malicious activity.
- To keep your DNS server secure, secure DNS makes it so that only members of an Active Directory domain can create records on the DNS server.

Summary

- Since the computer is connected to an organization’s network which may have direct and indirect access to servers and the network resources, it is important to protect the client computer.
- Some viruses, worms, rootkits, spyware and adware are made possible because they exploit some security hole within Windows, Internet Explorer or Microsoft Office.
- The first step that you need to protect yourself against malware is to keep your system up-to-date with Windows (as well as other Microsoft products such as Internet Explorer and Microsoft Office) with the latest service packs, security patches and other critical fixes.

Summary

- User Account Control (UAC) is a feature that started with Windows Vista and is included with Windows 7 that helps prevent malware.
- Microsoft recommends that you should always use the Windows Firewall.
- Simple Mail Transfer Protocol (SMTP) is used to transfer email from one server to another and it is responsible for outgoing mail transport.
- Spammers look for unprotected SMTP servers to relay their email through.

Summary

- To help manage Internet Explorer security when visiting sites, Internet Explorer divides your network connection into four content zones or types. For each of these zones, a security level is assigned.
- Phishing and pharming are forms of attacks to get users to a bogus website in an attempt to spread malware or collect personal information.

Summary

- To secure a server is to harden the server where you reduce the surface of attack and you reduce the server’s vulnerabilities. To harden a server, you should look for security guides and best practices for Windows servers and for the specific network services that you are installing.