Lesson 8: Protecting Yourself Online

Objectives

By the end of this lesson, you will be able to:

- 1.5.5: Define the function of Secure Sockets Layer (SSL), Transport Layer Security (TLS) and other encryption methods in securing communication for various protocols (e.g., FTP/FTPS, HTTP/HTTPS, IMAP/IMAPS, POP3/POP3S).
- 1.9.2: Identify advantages and disadvantages of using cookies, and set cookies, including setting a cookie without user knowledge, automatically accepting cookies versus query, remembering user actions, security and privacy implications.
- 1.10.1: Define the three major types of encryption.
- 1.10.2: Identify ways that authentication, digital certificates, encryption and firewalls provide Web security.
- 1.10.3: Identify ways that encryption helps enforce data confidentiality, data integrity and non-repudiation to secure end-user transactions.
- 1.10.4: Describe a computer virus and explain how to protect your computer from virus attacks.
- 1.10.5: Explain the functions of patches and updates to client software and associated problems, including desktop security, virus protection, encryption levels, Web browsers, e-mail clients.
- 1.10.6: Identify steps to take when you receive an unexpected attachment (e.g., via an e-mail or instant message client).
- 1.10.7: Identify steps to take when an attack is suspected.
- 1.10.9: Lock a computer to increase workplace security.
- 1.10.10: Distinguish between a virus and a worm.
- 1.10.11: Demonstrate the functionality of spyware.
- 1.10.12: Define the practice of typosquatting.
- 1.14.1: Define privacy concerns.

- 1.14.2: Identify appropriate use of company and personal systems.
- 1.14.3: Summarize personal privacy expectations versus an organization's right to know how its provided services are being used.
- 1.14.4: Identify basic copyright issues.
- 1.14.5: Explain the purpose of encrypting company transmissions and establish company encryption policies.
- 1.14.6: Discuss "The Right to Be Forgotten" and the possible ramifications of damaging posts on the Internet.

Pre-Assessment Questions

1. What is the most secure method for sending information over the Internet?

   a. Using encryption
   b. Using passwords
   c. Using patches
   d. Using spyware

2. What is malware?

   _____

   _____

   _____

3. What is a cookie?

   a. A harmful piece of code
   b. A helper application
   c. A published privacy policy
   d. A small text file

Introduction to Protecting Yourself Online

OBJECTIVE
1.14.1: Privacy issues

1.14.2: Appropriate use issues

1.14.3: Personal privacy vs. company resources

1.14.6: "The Right to Be Forgotten"

One of the major drawbacks of networked computing and Internet use is that your computer activities and personal information are no longer private. For example, online businesses collect information from users who make purchases on the Internet, and may sell the information for advertising or marketing purposes. Social networking sites such as Facebook and others specialize in profiting from information gathered on their platforms, even if they do not sell information to third parties. While these practices are not necessarily nefarious, they do have implications regarding your privacy.

CIW Online Resources – Movie Clips

Visit CIW Online at http://education.Certification-Partners.com/CIW to watch a movie clip about this topic.

Lesson 8: Protecting Yourself Online

The Right to Be Forgotten

You are ultimately responsible for protecting your image and personal information in the world of social networking. Think about the possible ramifications of posting personal information. Many employers search the Internet for information on potential employees. If you have posted damaging information, such as an incriminating photos or offensive jokes, it can be difficult to remove once the data is acquired by a search engine. Posted information can lead to damaged reputation and identify theft.

"The right to Be Forgotten"
An argument that asks "Do people have the right to remove damaging information about themselves on the Internet so the information can be forgotten?"

A phrase has arisen called "**The Right to Be Forgotten**." Do people have the right to remove damaging information about themselves on the Internet so the information in question can be forgotten? Several lawsuits have been filed to remove such information. For example, a cosmetic surgeon in Spain was sued by a woman who claimed he botched her procedure. A news report was posted stating the surgeon was sued for malpractice. The lawsuit was thrown out by the court because it was frivolous.

However, when people searched for the plastic surgeon using a search engine, the news article continued to appear next to his business' search result. Although the lawsuit was dismissed, a news story was never posted stating that the suit was thrown out. In an effort to protect his reputation and business, the surgeon sued Google in an effort to remove the news story from the search results. He lost the suit and the information remains to this day.

Do people have the right to have their information removed from the Internet once it is picked up by a search engine? This issue will be argued for years to come.

OBJECTIVE
1.14.1: Privacy issues

1.14.2: Appropriate use issues

1.14.3: Personal privacy vs. company resources

Spam

When you communicate with others via the Internet, whether you are on a PC, smartphone or tablet, your system can encounter various issues. For example, you may find that your system has become infected by malware, or you may become the recipient of spam sent via text messages or e-mail . Because spam is sent to you uninvited, it can be considered an invasion of privacy. And even though spam generally has no harmful effects on computer systems, reviewing and deleting the unwanted messages may hinder your productivity.

Some actions you can take to minimize the spam you receive include the following:

NOTE: The actions listed here can also protect users from being victimized by unauthorized users, malicious attackers and malware.

- **Avoid adding yourself to unwanted mailing lists** — When you submit any type of online form, choose to not be added to a mailing list (unless you want to be added to the list). If such an option is not available, consider not submitting the form.
- **Conduct online transactions through secure Web sites** — Before you purchase anything over the Internet, ensure that the transaction is secure. Most browsers will inform you whether a site is secure when you access the site. Remember that a URL beginning with *https://* ensures that your Web session is managed by a secure protocol, which encrypts and decrypts the information you send and receive during the course of the transaction.
- **Do not assume that only the intended recipient will read your messages** — Assume that whatever you write in an e-mail message could be seen by other people, particularly if you work for a company that routinely monitors its employees' text messages or e-mail messages. Even if your company does not monitor communications, the person to whom you send a message may forward it to others with your original message intact.
- **Be selective when posting information to newsgroups** — Remember that many social networks and chat rooms are unsupervised. When you post a message to a social network, your message becomes available to all those who have access to your profile, which can make you vulnerable to unwanted solicitations or virus attacks. Before posting any messages, monitor the social network to determine whether the users seem trustworthy. Check your privacy settings to see who can access your messages.

NOTE: Consider instances in which corporate monitoring is appropriate and when it is inappropriate. What do you think about such a policy?

Some organizations monitor the messages their employees' send and receive via e-mail, text message and social networks, and restrict their access to certain Web sites. Employers sometimes adopt such a policy because they consider all information carried by the company's communication system to be company property, just as the network, communication equipment and software used by the employees are company property. However, by restricting access to certain Web sites, companies may be denying employees legitimate Internet resources that may help them do their jobs.

Reasons that some companies elect to monitor employees' messages or restrict Internet access include the following:

- To protect proprietary information
- To prevent users from viewing or downloading undesirable data or malware
- To ensure that resources are being used solely for business purposes

Network administrators can also audit the contents of employee hard drives. Cached files from the Internet (as well as personal document files you have created) may be subject to examination. Therefore, you should use your home computer to keep personal data and send personal messages, and use company resources only for work-related activities.

For example, you may be trying to help a family member find a job. You may modify and format his or her résumé on your company computer, and spend time surfing the Web for employment-related sites. Are you using the resources provided to you for their intended purposes? Are you being paid to use company resources for personal business? Could the time you spend helping your family member be better spent on work-related tasks, which in turn help the business?

OBJECTIVE
1.9.2: Cookies

Cookies

As you learned in a previous lesson, cookies are small text files placed on Web site visitors' computers so that Web site managers can customize their sites to their visitors' preferences. For example, a cookie might be used to store information about your actions, such as the options you clicked on a Web page. Cookies are stored on any computer that uses a Web browser, including PCs, smartphones and tablets.

Cookies are sent to the client the moment a visitor accesses a Web site, and are usually used for identification. Cookies are connected to a database entry on the server site. These cookies enable the issuing cookie authority to customize distribution of its Web content to the visitor's operating system and browser.

Cookies can also be used to gather visitor information that could be used for marketing purposes, such as contact information (phone number, e-mail address or home address) or the operating system and browser you use. Unless you enter this personal information on a Web site, cookies do not have access to any data about you.

There are several different types of cookies. A persistent cookie is stored as a file on your computer and remains there after you end your browser session. A session cookie is stored only during the current browsing session and is deleted from your computer when you close your browser. A first-party cookie comes from the Web site you are currently viewing. A third-party cookie comes from a Web site other than the one you are currently viewing. Generally, third-party Web sites are sites that provide advertising content on the Web site you are currently viewing.

NOTE:
Cookies are safe. Because they are simple text files, they are harmless and very helpful when accessing sites you visit frequently that allow user preferences. If you did not have a cookie on your system for a site, you would have to customize your user preferences each time you visited it. Cookies are viewed as more of a privacy threat than a security threat.

If a user configures his or her browser to allow cookie downloads from Web sites, then each time the user revisits that site, the user's computer will send the cookie to the Web server. The cookie can inform the Web server of the visitor's preferences, such as selection for local news and favorite stocks, as well as the sections of the site the visitor has navigated. Once a cookie is saved on a computer, only the Web site that created the cookie can read it.

A persistent cookie is stored in a specific directory on your computer. Cookies are considered to be so useful to both end users and application developers that browsers allow them by default. However, most browsers allow you to control cookie functions. Depending on security settings, the browser can warn users before accepting a cookie, and then allow users to view, restrict or disable cookies completely.

CIW Online Resources – Online Exercise

Visit CIW Online at *http://education.Certification-Partners.com/CIW* to complete an interactive exercise that will reinforce what you have learned about this topic.

Exercise 8-1: Cookie types

Privacy issues with cookies

Web sites publish privacy policies in both human-readable form (which you can view on the Internet) and as a file that can be interpreted by your browser. For example, Internet Explorer looks for a compact policy, or a condensed computer-readable privacy statement, before accepting cookies.

A Web site's privacy policy should disclose the types of information the site collects, the ways that information may be used and the parties to whom that information may be given. Once your information has been collected, the site can use the information for its own purposes (which may or may not include sharing that information with others). Some sites will share your information without your consent.

After reading a Web site's privacy policy, you can decide whether you want to provide that site with your personal information. Consider that there is no guarantee that a Web site will adhere to its own published privacy policy.

Controlling cookies

In most browsers, you can control when and from whom cookies are accepted (called automatic cookie handling) by specifying the level of privacy you want to maintain. In Internet Explorer, use the Privacy tab of the Internet Options dialog box (shown in Figure 8-1) to control cookies.

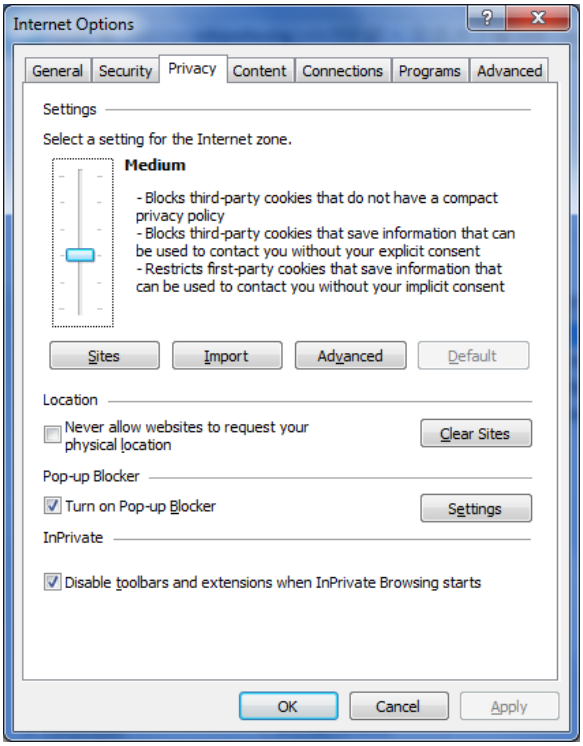

Figure 8-1: Controlling cookies — Windows Internet Explorer

You use the slider bar to adjust the level of privacy to your specifications. Table 8-1 shows the effects that each privacy level has on cookies.

Table 8-1: Internet Explorer Privacy level effects on cookies

Privacy Level	Effect on Cookies
Block All Cookies	Blocks cookies from all Web sites, and existing cookies on your computer cannot be read by Web sites.
High	Blocks cookies from all Web sites that do not have a compact policy, and blocks cookies from all Web sites that use your personal information without your explicit consent.
Medium High	Blocks cookies from third-party Web sites that do not have a compact policy and/or that use your personal information without your consent. Also blocks cookies from first-party Web sites that use your personal information without your consent.
Medium	Blocks cookies from third-party Web sites that do not have a compact policy and/or that use your personal information without your consent. Also deletes cookies from first-party Web sites that use your personal information without your consent when you close Internet Explorer.
Low	Blocks cookies from third-party Web sites that do not have a compact policy, and deletes cookies from third-party Web sites that use your personal information without your consent when you close Internet Explorer.
Accept All Cookies	Saves all cookies on your computer and allows existing cookies to be read by the Web site that created them.

You can configure your browser to override automatic cookie handling and instead display warnings, or accept or block first-party and third-party cookies. In Firefox, you can control whether or not to accept first-party or third-party cookies, or both, by selecting or deselecting cookie options on the Privacy panel of the Options dialog box (Figure 8-2).

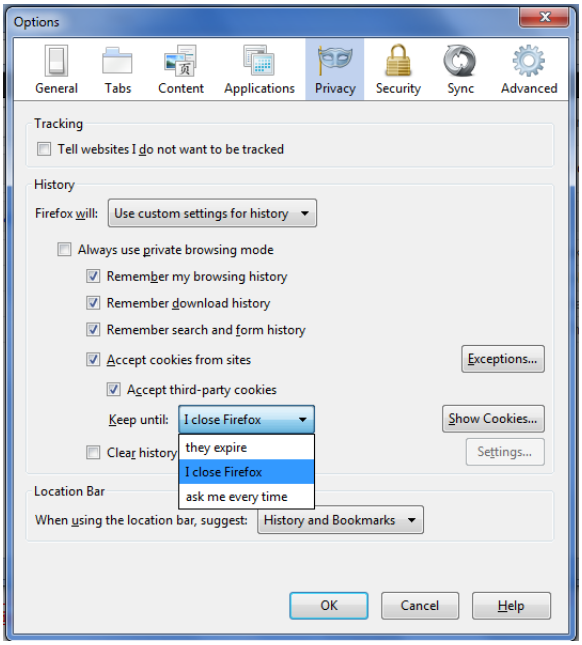

Figure 8-2: Controlling cookies — Mozilla Firefox

If you specify to accept cookies, you can use the Keep Until options (Table 8-2) to control the way cookies are handled.

Table 8-2: Cookie handling options — Firefox

Keep Until option	Effect on Cookies
They expire	Each cookie will be removed when the site determines the cookie will expire.
I close Firefox	Cookies will be deleted when you close Firefox.
Ask me every time	An alert will appear when a site tries to store a cookie.

Configuring your browser to prompt you when cookies are sent can show you how extensively cookies are used.

Viewing cookie content

You can view the file content of cookies sent to browsers. Cookie files are partially encrypted, so you will not be able to read them easily, but you can see information about the Web site that sent them to you.

In Firefox, you can view cookies and display information about them in the Cookies dialog box, shown in Figure 8-3.

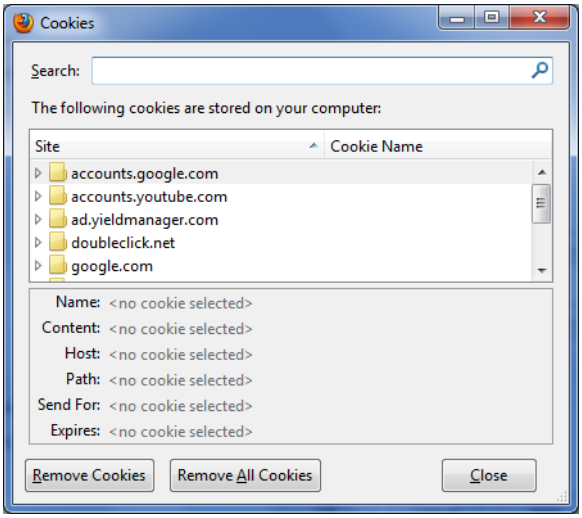

Figure 8-3: Cookies dialog box — Mozilla Firefox

In the following lab, you will configure Firefox to reject cookies, and then to display cookie warnings. Suppose a manager in your company has read that cookies store personal information, and he asks you to adjust his browser to reject all cookies. Suppose that the manager then complains that he cannot access various Web sites and cannot find information that he needs. You tell him that by setting his browser to display cookie warnings, you will demonstrate to him how useful and common cookies are.

Lab 8-1: Controlling cookies in Mozilla Firefox

In this lab, you will control the way cookies are handled by Firefox.

1. Open the **Firefox** browser.
2. Select **Firefox | Options**, then display the **Privacy** panel. In the History section, make sure that **Use Custom Settings for History** is selected in the Firefox Will drop-down menu.
3. Click the **Show Cookies** button, then click the **Remove All Cookies** button to delete the cookies you have so far accumulated. Click the **Close** button.
4. In the History section, deselect **Accept Cookies From Sites**, then click **OK**.
5. Go to the ***www.google.com***, ***www.CIWcertified.com*** and ***www.adobe.com*** Web sites.
6. Select **Firefox | Options**, ensure that the **Privacy** panel appears, then click the **Show Cookies** button to display the Cookies dialog box. Notice that although you have visited three Web sites since removing your cookies, no cookies appear.
7. Close the **Cookies** dialog box but keep the **Privacy** panel open.
8. Select **Accept Cookies From Sites**, then display the **Keep Until** drop-down list. Notice that there are three options to control the way cookies are handled.
9. Select **Ask Me Every Time**, then click **OK** to enable the new cookie settings. You now have the following options for handling cookies. You can specify that Firefox:
   - Accept a cookie.
   - Make the cookie a session cookie only (it will be deleted when the current Firefox session is over).
   - Reject a cookie.
10. To receive a cookie, visit a site not visited since you removed all cookies. For example, visit ***www.facebook.com***. A Confirm Setting Cookie dialog box similar to the one shown in Figure 8-4 will appear. Notice that the dialog box is prompting you to accept or reject a cookie for the Web site you want to visit.

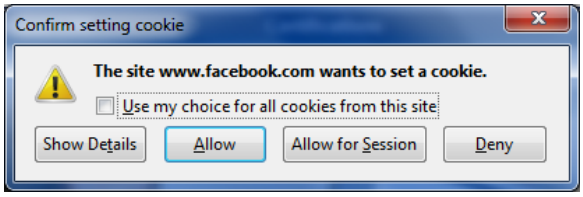

Figure 8-4: Confirm Setting Cookie dialog box — Mozilla Firefox

11. Select **Use My Choice For All Cookies From This Site**, then click the **Allow** button to accept the cookies.
12. Another Confirm Setting Cookie dialog box may appear. If it does, ensure that **Use My Choice For All Cookies From This Site** is selected, then click the **Allow** button

to accept the cookies. Depending on the site you visited, you may need to click the **Allow** button multiple times to accept all cookies associated with the page.

13. Select **Firefox | Options**, ensure that the **Privacy** panel appears, then click the **Show Cookies** button to display the Cookies dialog box. Notice the cookies that now appear in the Site list.

14. In the Site list, open a folder and select a cookie to display information about it, including its expiration date.

15. Close the **Cookies** dialog box but keep the **Privacy** panel open.

16. Display the **Keep Until** drop-down list, select **They Expire**, and then click **OK** to restore the original cookie setting.

17. Minimize the **Firefox** window.

OBJECTIVE
1.9.1: Browser preference configuration

Configuring Browser Security

You can configure your browser for added security by controlling active content that is downloaded from a Web site and run locally on the client's browser. The most common types of active content are JavaScript and ActiveX controls.

NOTE:
ActiveX controls and JavaScript are still used on the Web due to browser security improvements. JavaScript continues to grow in popularity with the advent of HTML5. Both ActiveX and JavaScript can provide a superior Web-browsing experience.

Both JavaScript and ActiveX controls allow information to be downloaded and run on your system. However, some content can cause problems ranging from inconvenience to data loss. Professional developers have created hostile ActiveX controls simply to demonstrate the possible security breaches. In response, browser vendors created safeguards to protect users. The danger is now remote, but you should know how to shield your system from active content.

To protect your system from incursions, browsers provide control options to enable or disable the execution of JavaScript or ActiveX controls.

Some corporate IT departments disable JavaScript and ActiveX on browsers used within the company. Disabling these features in a corporate environment can protect the corporate servers and computers from possible security compromises.

CIW Online Resources – Movie Clips

Visit CIW Online at http://education.Certification-Partners.com/CIW to watch a movie clip about this topic.

Lesson 8: Control your browser

OBJECTIVE
1.9.1: Browser preference configuration

Internet Explorer safety levels

Internet Explorer provides several settings that allow you to determine whether potentially dangerous content can be downloaded to your computer automatically, with a warning, or not at all. These settings will often determine whether you can download active content, such as ActiveX controls.

You use the Security tab of the Internet Options dialog box (Figure 8-5) to set safety levels in Internet Explorer.

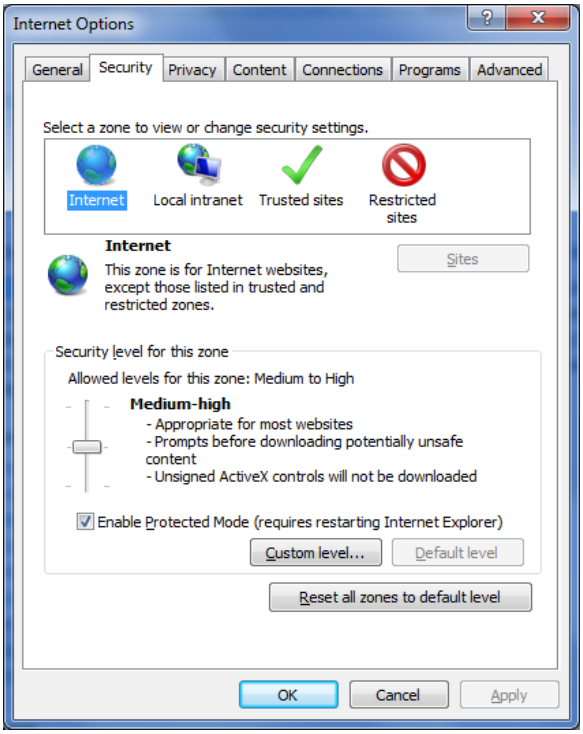

Figure 8-5: Internet Explorer Internet Options dialog box — Security tab

Each safety level performs certain actions or requests, depending on the content of the Web page. For example, if the High setting is selected and a Web page with ActiveX content is encountered, the active content will not display if the ActiveX control is not signed (you will learn more about digital signatures and certificates later in this lesson). An alert dialog box will appear instead. The High safety level does not give you the option to view the active content.

If the Medium-High safety level setting is selected, you may receive a warning message when you start to download a file. When you see such a message, you are given the option to open the file in its current location, save it to your hard drive, cancel the download or request more information.

If Medium is selected for the safety level, you will still be prompted when downloading potentially unsafe content and ActiveX controls, but more elements will be allowed through than with higher safety level settings.

If you are not denied access or prompted, then active Web content will download and operate in your browser automatically.

Firefox security

NOTE: Rather than supporting ActiveX, Firefox supports JavaScript.

Mozilla Firefox supports many of the same features as Internet Explorer, with the exception of ActiveX (ActiveX is a Microsoft-specific technology). Browser security settings are also handled differently in Firefox. You use Firefox's Options dialog box to disable features in order to configure browser security. You have already seen how to block pop-up windows and control cookies. You can use the Content panel of the Options dialog box to disable JavaScript, as shown in Figure 8-6.

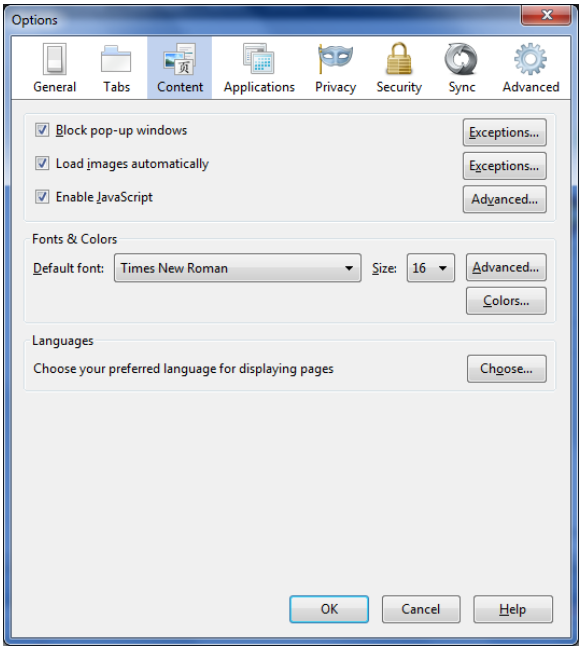

Figure 8-6: Enabling or Disabling JavaScript— Firefox

Java is a programming language that permits Web site designers to run applications on your computer. JavaScript is a scripting language used for client-side Web development and for enabling scripting access to objects embedded in other applications.

In the following lab, you will disable JavaScript in Firefox. Suppose your company's security manager has established a security policy stating that employees are to avoid downloading JavaScript when using the Web. You are assigned to ensure that this setting is put into effect on the browsers on all corporate systems. You can configure the security settings in Firefox to accomplish this.

Lab 8-2: Changing security settings in Mozilla Firefox

In this lab, you will change the security settings for downloading JavaScript with the Firefox browser. You must use a Firefox version that supports HTML5, such as 12 or higher.

1. Restore the **Firefox** window.
2. Go to ***http://html5demos.com/geo.*** Notice the JavaScript pop-up window that appears, as shown in Figure 8-7.

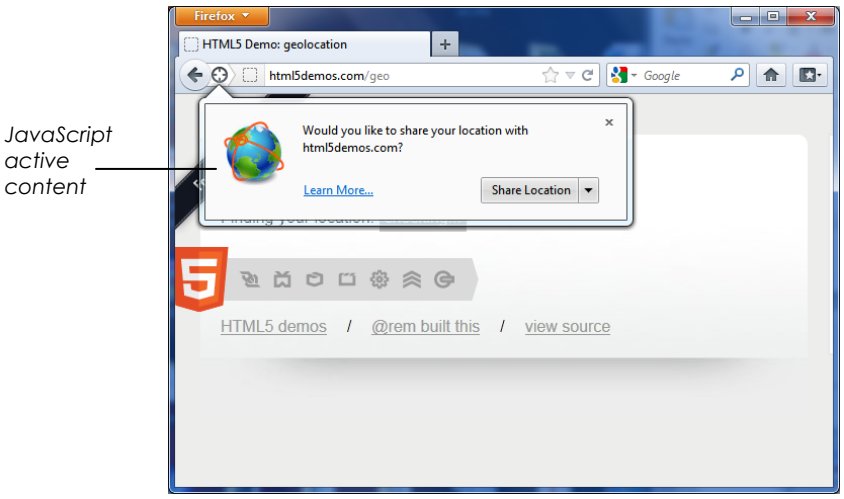

Figure 8-7: JavaScript active content

3. Just for fun, click **Share Location** to see if the HTML5 JavaScript application can locate you. If it cannot locate you, do not worry, the JavaScript code will download regardless.

4. Select **Firefox | Options**, then click **Content** to display the Content panel of the Options dialog box. Notice that Enable JavaScript is selected by default.

5. Deselect **Enable JavaScript** and click **OK**.

6. Right-click the Web page and select **Reload**. Notice that the JavaScript active content no longer appears. The page does not function.

7. Select **Firefox | Options**, select **Enable JavaScript**, then click **OK** to return the Content panel to its default settings.

8. Reload the page. Notice that the JavaScript active content reappears.

9. Minimize the **Firefox** window.

Safety levels are important for all Web users. With the rapid growth of the Internet, and the number of files and active programs transferred over it, security awareness has become increasingly important. You may find it disruptive to be warned for every cookie or active content item you encounter, but the warnings will serve as a constant reminder of the importance of Web security. Which security method will you use when you return to your workplace?

OBJECTIVE
1.10.2: Authentication, digital certificates, encryption, firewalls

Authentication

Authentication is the process of verifying the identity of a user who logs on to a computer system, or verifying the integrity of transmitted data. Before providing (or "serving") pages, servers require authentication. Browsers must be able to engage in the authentication process.

authentication
The process of verifying the identity of a user who logs on to a system, or the integrity of transmitted data.

General authentication types include the following:

- **Anonymous logon** — No user name or password is required, and authentication is handled automatically and transparently by the browser and the server. Whenever

you "hit" a site, an anonymous logon takes place, and the Web server will count each instance as an anonymous logon.

- **Basic authentication** — A user name and a password are required. You are prompted to enter your information before you can access the Web page, and that information is sent across the Internet as plaintext. Anyone who intercepts the data with packet-sniffing software will be able to read it.
- **Secure authentication** — A user name and password are required, and that information is encrypted before it is sent across the Internet, so that anyone who intercepts the data will not be able to read it. Encrypted authentication can be performed by various methods, which will be discussed shortly. In basic and secure authentication, knowledge of the user name and password are assumed to guarantee that the user is authentic.
- **Digital certificates** — You must have the proper digital certificate to gain access. A user name or password may not be required to access the site. Digital certificates will be discussed in detail shortly.

As you can see, authentication is usually performed through the use of digital certificates, and user names and passwords.

CIW Online Resources – Online Exercise

Visit CIW Online at *http://education.Certification-Partners.com/CIW* to complete an interactive exercise that will reinforce what you have learned about this topic.

Exercise 8-2: General authentication types

User names and passwords

Requiring user names and passwords is the most common way to authenticate users on private and public computer networks, including the Internet. User names and passwords provide a measure of Web security because the user must enter the correct user name and password to gain access to the Web server. However, user names and passwords can easily be forgotten, intercepted or accidentally revealed, which diminishes their reliability. To provide additional security, digital certificates are also used on the Internet for authentication.

OBJECTIVE
1.5.5: SSL/TLS and encryption protocols

Digital certificates

digital certificate
A password-protected, encrypted data file containing message encryption, user identification and message text. Used to authenticate a program or a sender's public key, or to initiate SSL sessions. Must be signed by a certificate authority (CA) to be valid.

A **digital certificate** proves the identity of an individual or company over the Web. A digital certificate is equivalent to an ID card and is digitally signed by the certificate creator.

Software developers use certificates to digitally sign the programs they develop. Digital signatures provide positive identification of the sending and receiving parties to ensure that programs downloaded from the Internet are original and safe. The browser can check the information in a certificate to see whether the program is valid or whether it has been tampered with since the certificate was signed. When you receive a certificate during a download, you can be relatively certain that the sender's identity is legitimate. You are offered the option to view the certificate, and you can cancel the download if you do not trust the authenticity of the sender of the digital certificate.

digital signature
An electronic stamp added to a message that uniquely identifies its source and verifies its contents at the time of the signature.

A digital certificate contains the requestor's name, a serial number, an expiration date, a copy of the requestor's public key and the digital signature of the certificate authority (so the requestor can verify that the certificate is legitimate). A **digital signature** is an electronic stamp that identifies a message's source and its contents. A digital signature can be used with any kind of content, encrypted or not.

Browsers allow digital certificate use; they enable you to obtain a personal certificate or a certificate for your business, and to view certificates from other companies.

The Web server administrator creates a digital certificate. The first step in creating a digital certificate is to create a certificate request. This certificate request is then signed by a trusted third party, called a certificate authority (CA). Commercial CAs such as Norton Secured Seal (previously VeriSign) (*www.symantec.com*) are organizations that verify the credentials of a server or company that has submitted a certificate request. Once the CA trusts the information provided by the party that submitted the request, the CA signs the certificate request, thereby creating a digital certificate.

The server always possesses the digital certificate. When a client begins an encrypted session, the server sends the certificate to the client. The client (Web browser or e-mail client) checks the signature on the certificate against its own list of CAs (which is loaded in your browser software). If the signature is recognized, then authentication occurs, because the client now knows that a trusted authority has verified the information provided by the server. After authentication occurs, encryption can begin.

non-repudiation
The security principle of providing proof that a transaction occurred between identified parties. Repudiation occurs when one party in a transaction denies that the transaction took place.

Digital signatures do not provide data confidentiality because they do not encrypt the data; they simply verify the integrity of the data and the identity of the sender. However, digital signatures enforce **non-repudiation**, which is the ability to prove that a transaction occurred. Sending data with a digital signature proves that the message was both sent and received. Neither party can repudiate the transaction.

Certificates provide a strong level of prevention against fraudulent use or misrepresentation of your personal or company information, and that of other Internet-based entities. Because the password method of authentication has inherent weaknesses (passwords can be stolen, forgotten or inadvertently revealed), the use of digital certificates seems likely to become the standard authentication method over the Internet.

CIW Online Resources – Online Exercise

Visit CIW Online at *http://education.Certification-Partners.com/CIW* to complete an interactive exercise that will reinforce what you have learned about this topic.

Exercise 8-3: Digital certificates

OBJECTIVE
1.5.5: SSL/TLS and encryption protocols

1.10.1: Major encryption types

1.10.2: Authentication, digital certificates, encryption, firewalls

1.10.3: Data confidentiality, data integrity, non-repudiation

Encryption

Most business Web pages encourage you to subscribe to, register for or purchase products or services over the Internet. These pages usually solicit personal or confidential information. If you submit information in a Web form, such as the form in Figure 8-8, how do you know that your personal data will be securely transmitted? Will a credit card number be stolen? Will a home address be exploited? Sending sensitive information across the Internet may seem unsafe. However, Web transactions are at least as secure as traditional transactions in which consumers give their credit cards to waiters in restaurants or supply credit card numbers to vendors over the phone. What prevents a waiter or a phone vendor from stealing the credit card number?

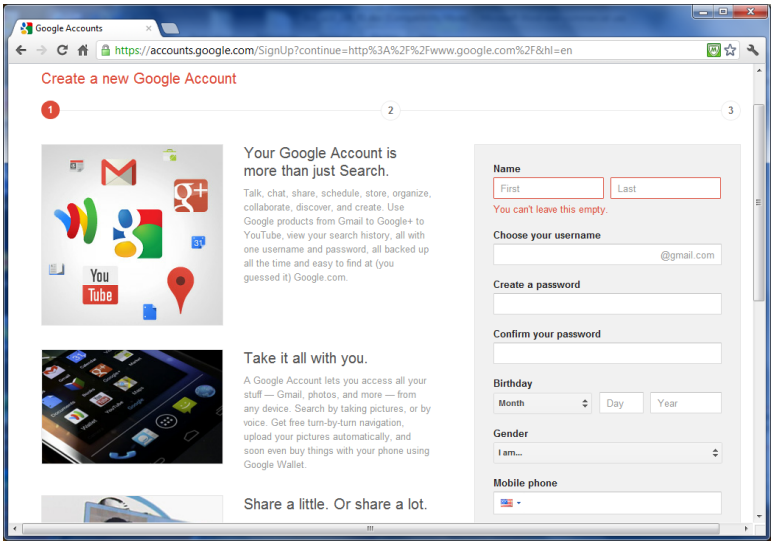

Figure 8-8: Web page personal information form

encryption
A security technique designed to prevent access to information by converting it into a scrambled (unreadable) form of text.

decryption
The process of converting encrypted data back to its original form.

In an effort to make online transmission of sensitive data more secure, many businesses use **encryption**. Encryption is the process of converting data into an unreadable form of text. Encryption is the primary means of ensuring data security and privacy on the Internet. For e-commerce businesses, the mere presence of encryption increases consumer confidence.

Decryption is the process of converting the encrypted data back to its original form. Encryption and decryption are performed through keys. A key is a mathematical algorithm. The more complex the encryption algorithm, the harder it is to decipher the encrypted message without access to the key.

Although encryption is often used in the process of authentication, it is not the same as authentication. Authentication occurs before an encrypted session can begin, but authentication does not ensure that the ensuing session will be encrypted.

Businesses use authentication and/or encryption for a variety of reasons. Generally, organizations use authentication to prevent unauthorized users from accessing company documents and data. Encrypted data transmissions prevent unauthorized users from intercepting and/or modifying data. Remember that the Internet is a public network, and people with malicious or criminal intent can intercept non-encrypted transmissions of data.

Encryption applications dramatically reduce the risk of information theft by scrambling the information using mathematical algorithms. Encrypted data is referred to as ciphertext; unencrypted data is referred to as plaintext.

key
A variable value, such as a numeric code, that uses an algorithm to encrypt and decrypt data. Some applications encrypt and decrypt with the same key, whereas other applications use a pair of keys.

Encrypted text cannot be read without the correct encryption **key**. Only the intended recipient of the information has the key to decrypt, or decipher, the data you supply. Because encrypted text is unreadable by anyone who does not possess the correct key, data encryption helps secure online transactions by ensuring the confidentiality and integrity of the data supplied by the sender.

Three types of data encryption exist:

- Symmetric encryption
- Asymmetric encryption
- Hash encryption

Symmetric (private-key) encryption

symmetric encryption
An encryption method in which the same key is used to encrypt and decrypt a message. Also known as private-key encryption.

Symmetric encryption (also called symmetric-key encryption or private-key encryption) is an encryption method in which the same key is used to encrypt and decrypt a message. The message sender uses a key (generated by an encryption application) to encrypt the message. Then the sender forwards a copy of the key to the message recipient, who uses the same key to decrypt the message. It is critical that the secrecy of the key be maintained by the sending and receiving parties in order for symmetric encryption to be effective. If the key is acquired by a malicious third party (such as during the key exchange between sender and recipient), the third party can use the key to decrypt the message and even pretend to be the message sender.

When you want to use symmetric encryption to communicate with your intended recipients, you should use asymmetric encryption (presented in the next section) to send the key.

For all encryption types, the 128-bit encryption standard is considered to be high-level encryption, although much more powerful keys exist (for example, 512-bit key standard).

Asymmetric (public-key) encryption

asymmetric encryption
An encryption method in which two keys (a private key and a public key) are used to encrypt and decrypt a message. Also known as public-key encryption.

Asymmetric encryption (also called asymmetric-key encryption or public-key encryption) refers to an encryption method in which two keys are used to encrypt and decrypt a message:

- **A public key** — The public key is known to all sending and receiving parties involved in the communication, whether via Web browsers, e-mail or instant messaging.
- **A private key** — The private key is used by the recipient to decrypt the message. Therefore, the private key must be kept secret.

NOTE:
Asymmetric (public-key) encryption is a far more secure encryption method than symmetric encryption.

The sending and receiving parties must share a public key in order to use asymmetric encryption. For example, when Sarah wants to send a secure message to Tina, Sarah uses a shared public key to encrypt the message. When Tina receives the message, she must use her own private key to decrypt the message. As long as Tina keeps her private key secure, only Tina will be able to decrypt her messages. When Tina wants to send a secure message to Sarah, Tina uses a shared public key to encrypt the message. When Sarah receives the message, she must use her own private key to decrypt the message.

In asymmetric encryption, the public and private keys are mathematically related so that only the public key can be used to encrypt messages, and only the corresponding private key can be used to decrypt them. Asymmetric-key encryption provides a high level of data confidentiality because it is nearly impossible for a malicious third party to decipher the private key, even if the third party knows the public key. Asymmetric encryption also provides a high level of data integrity because as long as the private key remains private, a malicious third party cannot alter the data before it reaches the intended recipient.

NOTE:
The RSA technology is so powerful that the U.S. government restricted exporting it to foreign countries during the 1990s. The ban has since been lifted.

The RSA algorithm

RSA is the most common asymmetric encryption algorithm. It was developed in 1977 by Ronald Rivest, Adi Shamir and Leonard Adleman. RSA is included in Web browsers and many other products. RSA (*www.emc.com/domains/rsa/*), which owns the encryption algorithm, licenses the algorithm technologies. RSA has evolved into the standard for Internet encryption, and is included in existing and proposed Internet, Web and computing standards.

Hash (one-way) encryption

hash encryption
An encryption method in which hashes are used to verify the integrity of transmitted messages. Also known as one-way encryption

hash
A number generated by an algorithm from a text string. Also known as a message digest.

Hash encryption (also called one-way encryption) is an encryption method in which hashes are used to verify the integrity of transmitted messages. (You learned about data integrity and data confidentiality in a previous lesson.) A **hash** (also called a message digest) is a number generated by an algorithm from a string of text. The generated hash value is smaller than the text itself, and is generated in such a way that it is nearly impossible for the same hash value to be generated from some other text. The hash is as unique to the text string as fingerprints are to an individual.

Hash algorithms are generally used to verify the validity of digital signatures (presented later in this lesson), which are used to authenticate message senders and recipients. The hash algorithm transforms the digital signature into a hash value. When a sender transmits a message, both the digital signature and the hashed digital signature are sent to the recipient, along with the message (which itself should be encrypted using symmetric or asymmetric encryption). The recipient's system then uses the same hash algorithm that the sender used; the recipient's application compares the digital signature to the sender's digital signature. If the hashed values are the same, the recipient can be confident that the message integrity remained intact. The hash algorithm verifies that the original message was not secretly decrypted, altered and re-encrypted during transit from sender to receiver.

Another use for hash encryption is to protect passwords from disclosure. A malicious third party cannot re-engineer the hash through a hash algorithm to decrypt a password. When a user enters a password to access a secure Web site or intranet, the password is encrypted and compared to the stored hashed password in the Web server. If the values match, then access is permitted. Once the password is hashed, the process cannot be reversed. Thus, hashing is always a one-way operation. Hash encryption is not useful for data confidentiality, because the encrypted data cannot be decrypted.

Hash algorithms: MD6 and SHA

NOTE:
MD stands for message-digest, another name for a hash.

Popular hash algorithms are MD2, MD4, MD5 and MD6. MD2, MD4 and MD5 are earlier versions of MD6, all of which were created by Ronald Rivest, one of the co-creators of the RSA algorithm. MD2 was optimized for 8-bit processors, while MD4 and MD5 were optimized for 32-bit processors. MD6 is optimized for 64-bit processors. The algorithms were intended to be used to encrypt and decrypt digital signatures, but they can be used to encrypt and decrypt messages of any length. MD5, which is the most popular version,

creates a 128-bit hash from the digital signature or message text. MD6, which is the most current version (introduced in late 2008), creates up to a 512-bit hash.

Another popular hash algorithm series is the Secure Hash Algorithm (SHA), which also creates hashes of up to 512 bits.

CIW Online Resources – Online Exercise

Visit CIW Online at *http://education.Certification-Partners.com/CIW* to complete an interactive exercise that will reinforce what you have learned about this topic.

Exercise 8-4: Data encryption methods

OBJECTIVE
1.14.5: Company encryption policies

Encryption policies

Encryption is a very effective safeguard, but the amount of protection it offers varies based on the type of encryption used and the size of the key. Smaller keys, such as 40-bit keys, are easier to break than 128-bit or 256-bit keys. However, longer keys require more computational power to encrypt and decrypt data, which can slow transmission. It is imperative that companies protect their encryption keys to ensure secure transmissions.

Many businesses encrypt network transmissions in order to:

- Protect data.
- Prevent data from being intercepted by malicious outsiders.
- Deter hackers.
- Respond to customer or competitor pressure for increased security.
- Comply with government requirements regulating the security of Internet data transmissions.

Even if data transmissions do not warrant encryption, network administrators may still need to protect the privacy of e-mail messages, which often contain information of a proprietary or confidential nature. As you have learned, Web browsers include S/MIME, which is based on RSA's asymmetric encryption algorithm. S/MIME describes the way that encryption information and a digital certificate can be included as part of the message body. Each e-mail message includes a digital signature, which the recipient must receive in order to decrypt the message.

Companies that conduct business internationally must be aware of the encryption laws in various countries. Some countries do not allow large encryption keys to be exported, which forces network administrators to implement encryption solutions that fall within legal guidelines.

When establishing company encryption policies, network administrators must determine the risk of sending unencrypted data based on the nature of the data and its risk to the company if it were obtained by unauthorized users. Encrypting data slows data communication because each packet of data must be encrypted and decrypted. If the data is proprietary or sensitive in nature, then encrypting transmissions becomes critical. If not, network administrators need not encrypt their transmissions.

OBJECTIVE
1.5.5: SSL/TLS and encryption protocols

Secure Sockets Layer (SSL) and Transport Layer Security (TLS)

Secure Sockets Layer (SSL)
A protocol that provides authentication and encryption, used by most servers for secure exchanges over the Internet. Superseded by Transport Layer Security (TLS).

Transport Layer Security (TLS)
A protocol based on SSL 3.0 that provides authentication and encryption, used by most servers for secure exchanges over the Internet.

Most servers use the **Secure Sockets Layer (SSL)** protocol for secure exchanges. The SSL protocol authenticates using digital certificates and provides for data encryption. Netscape originated SSL, and version 3.0 is the current standard. All major browsers support SSL 3.0.

Transport Layer Security (TLS) is the successor to SSL and is becoming more common. The Internet Engineering Task Force (IETF), which defines standard Internet operating protocols, developed TLS. Because TLS was developed by the IETF, you can read Requests for Comments (RFCs) about it. As you learned in an earlier lesson, RFCs are public documents of interest to the Internet community that include detailed information about standardized Internet protocols. RFCs are identified by number. RFC 2246 explains TLS 1.0. In contrast, no RFCs about SSL exist because it was developed by a private company.

SSL/TLS can be used to encrypt any type of TCP-based service (e-mail, instant messaging, Web/HTTP, FTP, etc.).

SSL/TLS sessions can use 40-bit encryption or 128-bit encryption. The size refers to the length of the session key generated by each SSL transaction. Again, the longer the key, the more difficult it is to break the encryption code. Most browsers support 40-bit and 128-bit SSL sessions.

In the United States and Canada, the use of 128-bit encryption is standard. Some countries restrict encryption strength to 40-bit, fearing that the use of 128-bit encryption might enable terrorists to conduct secure, unbreakable communications and evade authorities. The United States prohibits the export of encryption technology to seven nations that are considered threats.

OBJECTIVE
1.5.5: SSL/TLS and encryption protocols

Secure protocols

Various protocols in the TCP/IP suite (such as HTTP, FTP, IMAP and POP3) can be made more secure by running them over SSL. Secure protocols increase safety when sending sensitive data such as confidential company information or credit card numbers over the Internet, thus making e-commerce possible.

For example, HTTP over SSL (HTTPS) encrypts and decrypts information sent from the browser to the server, as well as information sent from the Web server.

Suppose you browse the Amazon.com site for a book about e-commerce security. While you are looking at Amazon's offerings, you are using HTTP. However, once you begin the process of purchasing a book online with a credit card number, you are sent to a Web page with a URL that starts with *https://*. When you submit (send) your credit card information to the server, your browser will encrypt the data transmission. The confirmation you receive from the server will also be encrypted and will display on a page with an *https://* URL. Your browser will decrypt the information and display it for you.

FTP over SSL (S/FTP) provides a more secure mode of file transfer to and from FTP sites. You can also use e-mail protocols (SMTP, POP3, IMAP) over SSL for more secure e-mail.

Internet Explorer and Firefox allow you to view information about sites that use secure protocols. When you visit a secure site, the site sends you its digital certificate. In addition to displaying the *https://* protocol in the Address bar, Internet Explorer displays a lock icon in the Address bar. You can click this icon to view details about the digital certificate and encryption. Firefox displays the Web site domain name to the left of the address bar. Click this domain name to view details about the secure session.

In the following lab, you will verify that Firefox supports the SSL 3.0 and TLS 1.0 protocols. Suppose that your company is considering using Mozilla Firefox as its default browser, and your IT supervisor has asked you to determine which protocols Firefox supports for secure exchanges. How would you determine this information?

Lab 8-3: Viewing the default Firefox protocols

In this lab, you will view the default protocols that Firefox supports for secure exchanges.

1. Restore the **Firefox** window.
2. Select **Firefox | Options** to display the Options dialog box.
3. Click **Advanced** to display the Advanced panel, and then click the **Encryption** tab. Notice that the Use SSL 3.0 and Use TLS 1.0 check boxes are selected (Figure 8-9), indicating that both protocols are used by Firefox by default.

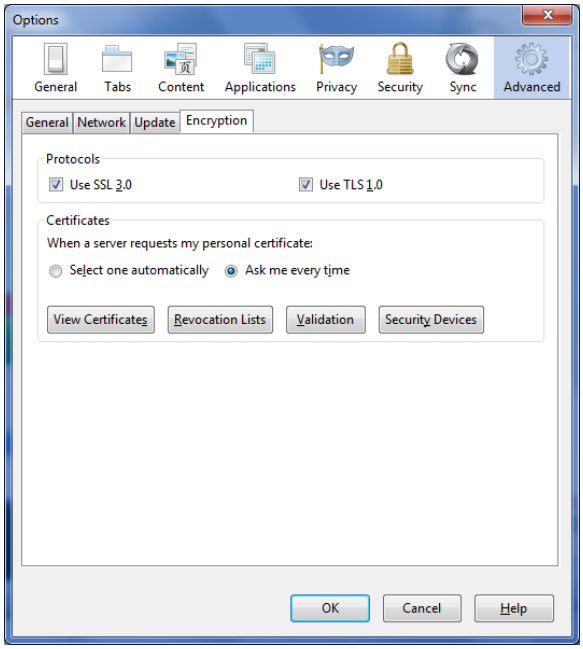

Figure 8-9: Default protocols — Firefox

4. Close the **Options** dialog box, then minimize the **Firefox** window.

CIW Online Resources – Course Mastery

Visit CIW Online at *http://education.Certification-Partners.com/CIW* to take the Course Mastery review of this lesson or lesson segment.

IBA Lesson 8 - Part A

Malware (Malicious Software)

malware
Abbreviation for malicious software. Malware is software designed to harm computer systems.

Malware, or malicious software, refers to programs or files whose specific intent is to harm computer systems. Malware is an electronic form of vandalism that can have global implications. You must be aware of malware to be able to detect and remove malicious code before it causes harm to your systems and networks. Malware includes computer viruses, worms, trojans and illicit servers, each of which will be discussed in this section.

CIW Online Resources – Movie Clips

Visit CIW Online at http://education.Certification-Partners.com/CIW to watch a movie clip about this topic.

Lesson 8: Scanning for malware

OBJECTIVE
1.10.4: Computer virus attacks

Viruses

virus
A malicious program that replicates itself on computer systems, usually through executable software, and causes irreparable system damage.

A **virus** is a malicious program designed to damage computer systems, from stand-alone computers to entire networks. Specifically, a virus is a program that assumes control of system operations, and damages or destroys data. Viruses are loaded onto your computer without your knowledge and run without your consent. All computer viruses are man-made and are often designed to spread to other computer users through networks or e-mail address books.

Viruses can be transferred via text or e-mail attachments, program or file downloads, flash drives, and social networking sites. In most cases, the creator or user of the source media containing the virus is unaware of its presence. For example, a virus might have written itself onto every flash drive that you used. If you pass an infected drive to a colleague, that colleague's system can also be infected. Similarly, a colleague might inadvertently send you an e-mail attachment infected by a macro virus. If you attempt to open or print the file, the virus will engage.

NOTE:
In general computer terminology, virus is used to refer to all malware (viruses, worms, trojans and illicit servers).

Viruses that reside within the text of an HTML-formatted message are particularly virulent because the user need only receive the virus for it to cause damage. The next time the virus recipient starts the computer, the virus runs and is sent to everyone in the recipient's address book.

A simple virus can:

- Display harmless messages on the screen.
- Use all available memory, thereby slowing or halting all other processes.
- Corrupt or destroy data files.
- Erase the contents of an entire hard disk.

Well-known virus examples

More dangerous viruses can have devastating effects on a global scale. Consider some well-known examples:

- **The Chernobyl (CIH) virus** — This virus infected Windows executable files, which caused computers to lose their data. In Korea, it affected approximately 1 million computers and caused more than US$250 million in damage.
- **The VBS Love Letter virus** — This virus overwrote Windows files with common file name extensions (such as .gif and .ini) on remote and local drives, replaced the files'

contents with the source code of the virus, and appended the .vbs extension to the files. All infected files were destroyed.

- **The Melissa virus** — This virus infected Microsoft Word documents and was sent to the first 50 people in each recipient's Microsoft Outlook Address Book. The virus inserted text into infected documents once every hour after the number of minutes corresponding to the date had passed (if the document was opened or closed at the appropriate time).

OBJECTIVE
1.10.10: Virus vs. worm

Worms

worm
A self-replicating program or algorithm that consumes system resources.

A **worm** is a self-replicating program or algorithm that consumes system and network resources. The difference between a worm and a virus is that a worm automatically spreads from one computer to another, whereas a virus requires some form of action from an end user, administrator or program. A worm can reside in active memory and replicate on the network. Sometimes a worm changes system files; sometimes a worm deposits a payload, which can be an illicit server or trojan. Worms can spread to all computers connected to a network and are commonly spread over the Internet via e-mail attachments.

For example, the PE_Nimda.A-O worm was spread as an executable file attachment in e-mail messages. The PE_Nimda.A-O worm did not require a user to open the e-mail attachment; it exploited a weakness in Microsoft e-mail clients and executed the file automatically. As this worm has shown, TCP/IP networks are particularly vulnerable to worm attacks.

Worms rely on specific software implementations. For example, Win32/Melting.worm attacks only Windows systems running Microsoft Outlook. This worm can spread by itself and can disable any type of Windows system, making it permanently unstable.

The Stuxnet worm was used to attack industrial software and equipment developed by Siemens. The worm was designed for the Windows operating system. Variants of the worm were used in cyber-warfare attacks against suspected uranium-enrichment facilities in Iran. Duqu, another worm, and Flamer, a malware toolkit, were also used for cyber-warfare attacks on various nations. The source of these powerful tools is unknown, but security professionals believe only a nation-state would have the resources to develop these highly complex devices. Expect more cyber-warfare between nations in the coming years.

Trojans

trojan
A program disguised as a harmless application that actually produces harmful results.

A **trojan** is a program that appears to be harmless but actually produces harmful results. They are named for the mythical Trojan horse that brought down the kingdom of Troy.

Trojans contain code that produces malicious or harmful results within applications that appear benign, such as computer games. Unlike worms and viruses, trojans do not replicate themselves or copy themselves to other files and disks. A trojan may be spread as part of a computer virus.

One of the most sinister trojan types is a program that claims to find and destroy computer viruses, but introduces viruses into your system instead.

Illicit servers

illicit server
An application that installs hidden services on systems. Illicit servers consist of "client" code and "server" code that enable the attacker to monitor and control the operation of the computer infected with the server code.

An **illicit server** is an application that installs hidden services on systems. Many illicit servers, such as NetBus and Back Orifice (a play on Microsoft's Back Office), are remote control or remote access programs.

Illicit servers differ from trojans in that they consist of "client" code and "server" code. The client (the malicious third party that is attacking a system) can send the server code as an unsolicited file attachment via e-mail, Internet chat and newsgroup messages to users, hoping that they will open the file and install the application. If the users who receive the server code install the application (intentionally or otherwise) and connect to the Internet, the attacker can use the client code's remote control capabilities to monitor and control the operation of the infected computers.

NOTE:
The term trojan comes from Homer's Iliad, in which the Greeks presented as a gift to the Trojans a large wooden horse, ostensibly as a peace offering. When the Trojans brought the horse inside the city walls, Greek warriors emerged from the horse and captured Troy.

An illicit server can be made to look like a patch or a program fix (which will be presented later in this lesson), so that recipients think they have received a legitimate file. Attackers can use illicit servers to perform malicious operations on infected computers, such as:

- Creating custom startup messages.
- Editing the Windows registry files.
- Sending messages.
- Changing the Desktop display.
- Playing sounds.
- Switching off the display screen.
- Disabling keyboard keys.
- Hiding the mouse cursor.
- Hiding the taskbar.
- Stealing passwords.
- Monitoring keystrokes.
- Restarting the computer.
- Locking up the computer.
- Executing applications.
- Viewing the contents of files.
- Transferring files to and from the computer.

CIW Online Resources – Online Exercise

Visit CIW Online at *http://education.Certification-Partners.com/CIW* to complete an interactive exercise that will reinforce what you have learned about this topic.

Exercise 8-5: Malware (malicious software)

Virus Detection and Prevention

NOTE:
The term virus in this context and throughout this course refers to all malware.

Corporate IT departments are often the first line of defense against computer viruses. Generally, the IT department will receive warnings about viruses that are being spread, and will have time to prepare for virus detection and subsequent disinfection. But many times individuals must protect themselves without any help.

Common ways that computer viruses are contracted include:

- Receiving an infected disk/drive from someone else and reading it from your disk drive.
- Downloading an infected file or program to your computer from a network computer, an intranet or the Internet.
- Downloading an illicit server attachment from a malicious source.
- Copying to your hard disk a document file infected with a macro virus.

OBJECTIVE
1.10.4: Computer virus attacks

Following are some actions you can take to protect your systems from contracting viruses:

- Do not open e-mail messages or attachments from unknown senders. This includes text messages.
- Configure the security settings for your e-mail program, Web browser and social networking sites to the highest possible levels you can tolerate.
- Use an anti-virus software program to scan flash drives, e-mail attachments, files, programs, software or disks (even new software from a trusted source) before you open or use them on your computer.
- Use an anti-virus software program to scan your disks and files if you use them on another computer.
- Use an anti-virus software program to scan all files and programs you download from the Internet.
- Keep your anti-virus software current by downloading virus signature updates as they become available.
- Stay informed about the latest virus threats so that you recognize an e-mail virus before you open and unleash it.
- Make backup copies of important files and store them on separate disks so that the files will be unaffected if you contract a virus.

Anti-virus software

anti-virus software
Software that scans disks and programs for known viruses and eliminates them.

The best protection against a virus is to know the origin of each program or file you install on your computer, or open from your e-mail or instant message client. Because this is difficult, you should use **anti-virus software** to scan e-mail attachments and files for known viruses, and eliminate any it finds.

In general, viruses can be detected when they modify parts of your system in order to pass themselves along. When a virus has been detected, you must use anti-virus software to disinfect your system. Anti-virus software that is kept current knows the signatures of viruses, and works by scanning the infected file or program for the identifying signatures. If the virus is found, your hard drive can often be disinfected immediately so that the virus cannot infect other files or cause more damage. Most anti-virus programs download

signature profiles of new viruses automatically so that the program can check for the new viruses as soon as they are discovered.

If your company has an IT department, it will probably provide and update anti-virus software for you. If you work for a company without an IT department, you can download anti-virus software from many Web sites. Trend Micro (*www.trendmicro.com*), McAfee, Inc. (*www.mcafee.com*) and Panda Security (*www.pandasecurity.com*) are three providers of anti-virus software. Another anti-virus software company, Symantec (*www.symantec.com*), provides the Symantec Security Response page (*www.symantec.com/security_response*), which identifies the latest virus threats. You can also obtain information about virus threats at the Trend Micro Security Information page (*http://about-threats.trendmicro.com/threatencyclopedia.aspx*). All of these Web sites are excellent sources of information about current viruses.

OBJECTIVE
1.10.6: Unexpected e-mail attachments

Unexpected attachments

Because attachments are the most common method for spreading viruses, you should be wary of any unexpected attachments you receive with e-mail, text or instant message transmissions.

Following are some actions you can take if you receive an attachment you did not expect or do not recognize:

- Do not attempt to open the attachment.
- Try to contact the message sender and determine whether the attachment is legitimate. (Consider that if the sender's e-mail address has been spoofed in order to send dangerous attachments to unsuspecting recipients, it is best to contact the sender via some method other than e-mail, to avoid a spoofed response from a determined attacker.)

NOTE:
Remember that when attachments are deleted from messages, the attachments are still in your system until you remove them from your Deleted Items folder.

- If you are unable to contact the sender or the sender is unaware of the attachment, delete the attachment from the message.
- Open your Deleted Items folder and delete the attachment from it to permanently remove the attachment from your system.

Virus attacks

If your computer is attacked by a virus, do not panic. Most viruses can be removed without permanent damage to your system, and most viruses can be halted even after they commence an attack.

OBJECTIVE
1.10.7: Suspected attacks

Following are some actions you can take if you suspect a virus attack:

- Use anti-virus software to remove the virus immediately.
- If the virus is active in memory and you are not able to launch the anti-virus software, turn off your computer and reboot from a known, clean system disk. This procedure will start the system without the virus in memory. You should then be able to launch the anti-virus software and begin the disinfection process.
- Check all your disks and backup files with the anti-virus software, and remove the virus from them if necessary.
- If files or programs are damaged or altered by the virus, you will need to replace them with backup copies or reinstall programs from original installation media.

- Because viruses can self-replicate, you must find and remove all copies of the virus in your system. Use the anti-virus software to scan your entire system and disks for the virus and remove it.
- If damage is widespread, you may be forced to reformat your hard disk and reload all your programs and files. However, this technique should be used as a last resort because most anti-virus software is very effective at disinfecting systems, even for difficult-to-remove viruses.

OBJECTIVE
1.10.11: Spyware.

Spyware and Virus Removal

spyware
A software application secretly placed on a user's system to gather information and relay it to outside parties, usually for advertising purposes.

Spyware (or adware) is a software application that is secretly placed on a user's system to gather information and relay it to outside parties, usually for advertising purposes. Many Internet-based applications contain spyware. Companies with both good and bad reputations have included spyware code in their software. Spyware can also be placed on a user's system by a virus or by an application downloaded from the Internet.

Once installed, spyware monitors the user's activity on the Internet and conveys the information to the spyware originator. The originator can then gather Web site usage, e-mail and even password information from the user, then use it for advertising purposes or malicious activities.

Spyware is analogous to trojans in that it is installed automatically without the user's knowledge or consent. Legitimate data-collecting programs that are installed with the user's knowledge are not considered spyware, as long as the user provides consent, and knows the type of data being collected and to whom it is being conveyed. For example, cookies are text files that store information about Internet use and reside on users' systems. Users generally know about cookies and their functions, and users can disable outside access to cookie information.

Spyware can also affect the efficiency and stability of computer operations by consuming memory resources and bandwidth. Because spyware is an independent executable program, it has the ability to:

- Scan files on hard drives.
- Read cookies.
- Monitor keystrokes.
- Install other spyware applications.
- Change the default home page in Web browsers.
- Automatically send information to the spyware developer.

Removing spyware helps ensure privacy by preventing companies from tracking your Internet activity and collecting your personal information.

CIW Online Resources – Online Exercise

Visit CIW Online at *http://education.Certification-Partners.com/CIW* to complete an interactive exercise that will reinforce what you have learned about this topic.

Exercise 8-6: Spyware

NOTE:
It is importance to make sure that so-called spyware removal applications are not trojans. Such applications may themselves contain spyware.

Detecting and blocking spyware

You can detect the presence of spyware by obtaining a spyware detection application. Such applications work much like anti-virus applications in that they scan a computer's hard drive, memory and network connections, and look for suspicious activity. These applications can be updated, just like an anti-virus application can be updated.

Network and systems administrators can detect the presence of spyware by doing the following:

- Using a network analyzer to capture and study network transmissions for suspicious packets.
- Using the netstat application to review all ports. (Netstat is a TCP/IP utility that reads network data structures.) If the administrator finds a suspicious port open on your system, he or she can conduct a Web-based search on that port. The administrator may discover that it is a port used by spyware installed on your system.

NOTE:
Detecting spyware via network analyzers and netstat are beyond the scope of this course. Network analyzers and netstat are introduced in the third coursebook of the CIW Web Foundations series, *Network Technology Associate*.

You can combat spyware by:

- Deleting the application that contains the spyware.
- Using a desktop firewall to block transmissions between your system and the spyware vendor.

Spyware-detection applications and false positives

Spyware-detection applications use the following strategies:

- They contain lists of known spyware.
- They contain programming that can detect suspicious activity, which includes Windows registry entries that are out of place, suspicious network connections, and applications that behave suspiciously.

Spyware-detection applications can report false positives, in which legitimate applications are incorrectly categorized as spyware. As you use a spyware-detection application, ensure that you examine the results carefully so that you do not remove legitimate applications.

In the following lab, you will install the Ad-Aware anti-virus and anti-spyware software. Suppose you are the IT administrator for a small family-run business. Several employees have complained that their default Web browser home pages have been changed without their input, and their computers have been running more slowly than they usually do. You suspect that they are victims of viruses and spyware, so you install anti-virus and anti-spyware software to find and remove the threats.

Lab 8-4: Installing and using anti-virus and anti-spyware software

In this lab, you will install and use Ad-Aware software.

1. Open **Windows Explorer** and navigate to the **C:\CIW\Internet\Lab Files\Lesson08** folder.
2. Double-click **Adaware_Installer.exe**. If you are asked if you want to allow the program to make changes to this computer, click **Yes**.

3. The language choices for setup should appear. Select your language for the installation and click **OK**.

   Warning: *If you receive a compatibility warning due to existing anti-virus software, uninstall or remove your existing anti-virus software. Serious issues will arise if you run two anti-virus programs at the same time. Your system will run extremely slow, become non-responsive, and this lab will not work.*

4. The Ad-Aware installation wizard will appear. Accept the agreement and click **Next**.

5. In the Ad-Aware Safe Browser Add-On window, deselect any additional software the program wants to install. You will only use the anti-spyware feature. Follow the installation instructions in the wizard to install Ad-Aware on your system. When the installation is complete, click **Finish** and restart your computer.

6. Upon reboot, Ad-Aware will automatically run a scan of your system in the background to detect any existing spyware on your system. This may slow down your system.

NOTE:
It may take a few minutes for the scan to finish and the Thank You window to appear.

7. A Thank You window will appear and ask you to unlock the Pro version. Do not upgrade. You will use the 30-day trial version for this lab. Close the **Thank You** window.

8. The Ad-Aware home page should appear automatically. If not, double-click the **Ad-Aware** shortcut on the Desktop to launch the application. The Ad-Aware window should resemble Figure 8-10.

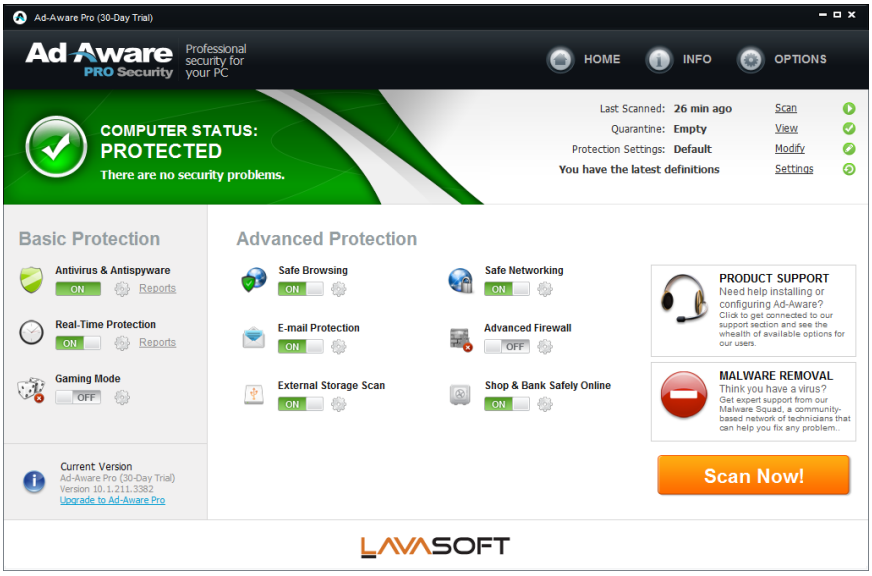

Figure 8-10: Ad-Aware spyware-detection application

NOTE:
Notice the Scan Now! options that lists the items to be scanned.

9. Click the **Scan Now** button. You can choose from among a Quick Scan, Full Scan or Custom Scan. A Quick Scan scans only the most critical sections of your system. A Full Scan will scan your entire system including all local drives. A Custom Scan will scan your system based upon pre-configured settings that you can specify.

10. Ensure that the **Quick Scan** tab is selected, then click the **Scan** button. Ad-Aware will perform an initial scan, which will look for viruses, spyware applications and suspicious activity.

Note: The scan may take several minutes, depending upon the size of your hard drive and speed of your system.

11. When the scan is finished, the Scan Results screen will appear. The Scan Results screen displays information about the scan you performed and information about the objects that were detected.

12. Notice the radio buttons that appear at the right end of each threat. Your screen should resemble Figure 8-11, depending on the scan results. Trojan threats were found in the scan shown in the figure.

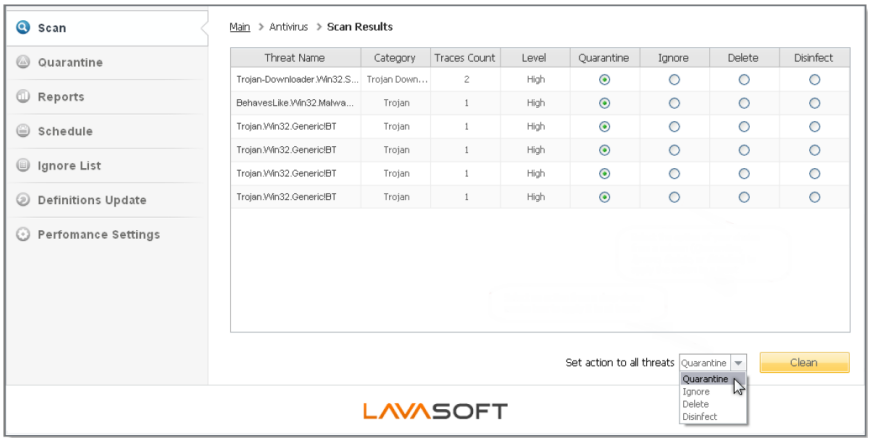

Figure 8-11: Virus threats detected — no spyware

13. Scroll through the list of objects. Notice that some objects may be selected for removal, others for quarantine, and so forth. If you notice any legitimate applications in the list, you are probably viewing false positives.

14. You can specify actions to perform on each threat using the radio buttons, or you can select an option in the Set Action To All Threats drop-down menu. Your choices are to:

- Delete the object from your system.
- Add the object to the Quarantine folder so that it does not pose a threat to your system.
- Add the object to the Ignore List so that it will not be detected during future scans.
- Disinfect/repair the object (available only for specific objects).

*Note: Do **NOT** click the Clean button, as this would perform the indicated actions, such as removing applications from your system or backing them up into a Quarantine folder. You do not want to remove or quarantine any applications in this lab unless you are absolutely certain they are harmful viruses or spyware.*

15. Close the **Ad-Aware** window without performing any action on the detected objects, unless there are harmful viruses or spyware on your system.

NOTE:
Take note of the Lavasoft Support URL, which you can use to access free online technical support and product information.

16. As a class, answer the following questions:

- Did you find any false positives?
- What viruses did you find?

- What spyware did you find?
- How can removing spyware improve privacy?

In this lab, you installed and used Ad-Aware spyware-detection software. For additional information about using Ad-Aware, including technical support, access the *www.lavasoftsupport.com/index.php* Web page.

OBJECTIVE
1.10.5: Client software patches and updates

Updates and Patches

update
A file or collection of tools that resolves system liabilities and improves software performance.

patch
Programming code that provides a temporary solution to a known problem, or bug.

An **update** is any file or collection of software tools that resolves system liabilities and improves software performance. A **patch** is a file of programming code that is inserted into an existing executable program to fix a known problem, or bug. Patches are designed to provide an immediate solution to a particular programming problem and can often be downloaded from the Web site of the software vendor. However, patches are intended to be only temporary solutions until problems can be permanently repaired.

Generally, a software vendor will provide permanent solutions to program bugs in later product releases, known as updates. Updates are released periodically when deemed necessary by the vendor. A major update with significant software improvements is often marketed as a new release.

Patches and updates should never be applied to all system units without applying them to test computers first. In fact, many security policies require an extensive testing process before an update is installed onto any systems. If the patches or updates do not address the problems your system is experiencing, or if there would be no performance gain by applying them, you should not install them. Patches and updates can cause incompatibility issues among system resources or applications, and can even introduce new security issues. However, if your system is vulnerable to a security problem, you may need to install the patches or updates as soon as possible.

Make sure that you obtain patches or updates from trusted sources, especially if the program is an open-source upgrade. Verify hashes and signatures before installing upgrades to avoid installing a virus onto your system.

Anti-virus program updates

Anti-virus program updates generally refer to files containing virus signature profiles that have become known since the last program update. Updates are important because even the best anti-virus program will not protect you if its signature profiles are outdated.

Anti-virus software uses signature profiles to recognize patterns that indicate viruses. Because new viruses are created so rapidly, manufacturers update these signature profiles frequently. Most anti-virus software will download the latest profiles automatically.

Encryption levels and Web browsers

Software applications and Web browsers support various encryption levels. Many Web sites require that your browser use 128-bit encryption for added security. Nearly all browsers support 128-bit encryption.

Desktop security

It is important to maintain the security of individual computers, particularly because most computers in the workplace are connected to corporate networks, intranets and the

Internet. Computers running older operating systems (such as Windows XP with Service Pack 2 or Windows Vista with Service Pack 1) are no longer supported with security patches, thereby leaving them vulnerable to intrusion. For newer computers (Windows 7 or later), it is important to apply regular operating system patches and updates supplied by software vendors to minimize security breaches.

E-mail clients

As you have already learned, e-mail is the most common way to spread viruses. You should keep your e-mail client current, and install necessary security patches and updates to minimize security breaches. Additionally, some e-mail clients default to 40-bit encryption levels. You can install updates to support 128-bit encryption if necessary.

OBJECTIVE
1.10.9: Locking a computer

Locking Your Computer

screen saver
A graphic or moving image that appears on your screen when your computer is idle.

A **screen saver** is a utility program that displays images or animation on your monitor when no keystrokes or mouse actions have occurred for a specified duration. You can use screen savers to hide your work while you are away from your desk, providing a measure of security. Some system screen savers allow you to password-protect your screen saver, which locks your computer. If you configure this feature, then once your screen saver activates to hide your Desktop, your specified password must be entered to deactivate the screen saver.

In Windows, you can use the Screen Saver Settings dialog box (Figure 8-12) to specify a screen saver and the amount of time your computer is to remain idle before the screen saver activates. You should also select the On Resume, Display Logon Screen check box for more security.

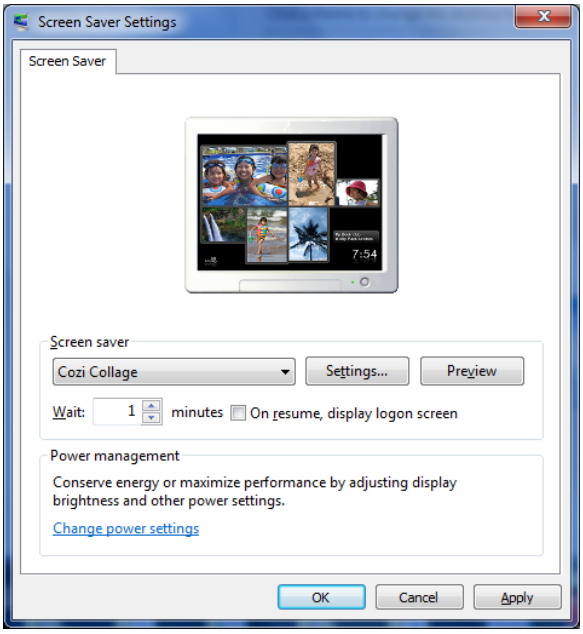

Figure 8-12: Screen Saver Settings dialog box

You do not have to wait until your screen saver activates to protect your system. To lock your computer quickly, press CTRL+ALT+DELETE and click Lock This Computer. When you return to the computer, you will be required to enter your logon information to access your Desktop again.

A dedicated hacker may simply steal your entire computer or try to guess your password, but in most cases, locking the screen will keep your system secure from physical threats.

In the following lab, you will lock your computer by activating a screen saver. Suppose you are an IT administrator and you want to update computer security measures in your company. One of the first tasks you perform is instructing employees to set their screen savers to display no longer than five minutes after their computers are idle, and to require a password to access the computer again.

Lab 8-5: Locking your computer by using a screen saver

In this lab, you will lock your computer by specifying a screen saver and the amount of time your computer needs to remain idle before activating it. A user name and password will be required to access the computer again.

Note: Only lock your computer if you have the password to this account. Otherwise, only activate the screen saver.

1. Right-click a blank area of the Desktop, click **Personalize** to display the Control Panel Personalization window, then click the **Screen Saver** link to display the Screen Saver Settings dialog box.
2. Display the **Screen Saver** drop-down list, then select a screen saver of your choice.
3. Double-click the contents of the Wait text box, then type ***1***. This step specifies that the screen saver will display when your computer has been idle for one minute.
4. To lock the computer when the screen saver activates, select the **On Resume, Display Logon Screen** check box. Skip this step if you do not have the account logon information. Click **OK**.

NOTE:
In Step 5, ensure that you do not engage in any activity with your computer for a full minute in order to make your screen saver activate.

5. Do not press any keys or move the mouse for at least one minute. The screen saver you selected should appear on your screen.
6. When the screen saver appears, move the mouse to display the logon screen. Press the **CTRL+ALT+DELETE** keys together, then enter the **password** to access the Desktop.
7. In the Control Panel Personalization window, click the **Screen Saver** link to display the Screen Saver Settings dialog box again.
8. Display the **Screen Saver** drop-down list, then select **3D Text**. To change the text, click the **Settings** button and enter the name of a company where you would like to work. Experiment with other settings and click **OK** when finished.
9. Double-click the contents of the Wait text box, then type ***10***. This step specifies that 10 minutes is the amount of time your computer needs to remain idle in order for the screen saver to activate.
10. Deselect the **On Resume, Display Logon Screen** check box. Click **OK** to close the dialog box.

11. Close the **Control Panel Personalization** window.

12. Now, press **CTRL+ALT+DELETE** and select **Lock This Computer** to immediately lock your screen. Experiment with your settings as needed.

OBJECTIVE
1.10.12: Typosquatting

Typosquatting

typosquatting
The unethical practice of registering domain names very similar to those of high-volume sites in hopes of receiving traffic from users seeking the high-volume site who mistakenly enter an incorrect URL in their browsers.

Typosquatting refers to an unethical practice in which the perpetrator (i.e., typosquatter) capitalizes on typing mistakes that users make when entering the URL of a Web site into a browser. Typosquatting is also known as URL hijacking. When a Web surfer accidentally enters an incorrect Web site address, he or she may end up viewing an alternative Web site owned by a typosquatter. Essentially, typosquatters are attempting to profit from a trademark belonging to another business by taking advantage of users' typographical errors.

Typically, a typosquatter will register several possible erroneous domain names for a frequently visited Web site. Then, the typosquatter will monitor the traffic received by the erroneous sites, and use the information to sell advertising to the sites receiving high volumes of traffic. The typosquatter might sell ads to the original site's competitors or redirect the user to related products or services.

The typosquatter's Web address will probably be very similar to the victim site's address; most typosquatting sites have domain names that have a one-letter difference from their victim's legitimate, trademarked domain. The address can be:

- A common misspelling of the victim's site.
- A foreign-language misspelling of the victim's site.
- A misspelling based on common typing errors, such as transposing two letters.
- A plural version of a singular domain name, or vice versa.
- A different top-level domain (e.g., *.net* instead of *.com*).

Some typosquatter Web sites may look almost exactly like the victim sites, or they may be completely different. Typosquatters frequently use their alternative sites to distribute adware, spyware, viruses or other types of malware.

When a Web site's owner determines that the site may be the victim of a typosquatter, he or she can:

- Send a cease-and-desist letter to the typosquatter, which is a request to halt the activity or face legal consequences.
- Bring a lawsuit against the typosquatter.
- Purchase the typosquatter's Web addresses.

Web site owners can also try to avoid falling victim to a typosquatter in the first place by purchasing domain names that are similar to their actual domain name. For example, the URLs *www.goooogle.com*, *www.goolge.com*, *www.gogle.com*, *www.gewgle.com* or *www.google.net* will all direct you to the Google home page at *www.google.com*.

Parked domains vs. typosquatting

An individual or a company can register a domain name not for the purpose of creating a Web site, but for the purpose of creating a page that contains advertising and links meant to help the company either sell the domain or make money from the links that are on the page. This type of domain is called a parked domain. If the page contains ads that net the registrant revenue, the parked domain is said to be monetized. Entire companies exist that attempt to sell parked domains.

Protecting Company Resources

The Internet is a network of shared information and resources. The connectivity that makes the Internet possible also makes systems vulnerable to unwanted activity. This section will identify Internet security issues that IT professionals must be familiar with in order to protect their companies' systems.

OBJECTIVE
1.10.2: Authentication, digital certificates, encryption, firewalls

Firewalls

A **firewall** is a security barrier that prevents unauthorized access to or from private networks. Businesses use this combination of hardware, software and corporate policies to prevent Internet users outside the business from accessing proprietary data on the business's networks that are connected to the Internet, as well as private intranets. Firewalls are also used to control employee access to Internet resources.

firewall
A security barrier that controls the flow of information between the Internet and a private network. A firewall prevents outsiders from accessing an enterprise's internal network, which accesses the Internet indirectly through a proxy server.

The most common business firewall technique uses a firewall server in conjunction with a proxy server to screen packets of data. All data entering or leaving an organization passes through the firewall. The firewall examines each packet and determines whether to forward it to its destination, based on security policies set up by the firewall administrator or IT department. The proxy server replaces the network IP address with another, contingent address. This process effectively hides the network IP address from the rest of the Internet, thereby protecting the network.

The need for firewalls

NOTE:
You can learn more about firewall functionality, topologies and security zones in the CIW *Network Technology Fundamentals* course.

When you connect your computer to the Internet, you are potentially connecting to all the computers on the Internet. This relationship works in reverse as well: All other computers on the Internet are connected to yours, and perhaps to all the computers on your corporate LAN.

Some LANs feature Web servers or FTP servers that provide confidential or proprietary files to users on the LAN. If the LAN is on the Internet, anyone outside the business who knows the domain name or IP address of the server could access these files. Often, these files have no encryption or password protection because the administrators of the Web or FTP servers did not know the LAN was accessible to the Internet.

By connecting to the Internet through firewalls, no computer on the LAN is actually connected to the Internet, and any requests for information must pass through the firewall. This feature allows users on the LAN to request information from the Internet, but to deny any requests from outside users for information stored on the LAN.

NOTE:
Most Internet users will never know whether a firewall is used on their network. Firewalls are often transparent because they do not require special configuration on the client systems.

Challenges of firewalls

Firewalls can be inconvenient for business users who are protected by them. For example, users may be unable to access an external e-mail provider or to upload files to external servers. Some standardized Internet plug-ins, such as RealPlayer, cannot function through firewalls. Some of the new video plug-ins used on news Web sites are also unable to operate through firewalls. If your employer's firewall interferes with work you need to conduct on the Internet, you should work with your IT department's firewall administrators to achieve a level of protection that allows you to access necessary resources.

Security policies

NOTE:
The term firewall originated from firefighting, in which a firewall is a barrier established to prevent the spread of fire.

Security policies are a vital part of any firewall strategy. The policies created by firewall administrators govern who will be allowed external access, what information employees will have access to, how often passwords must be changed and so forth. Hardware and software alone cannot protect information from employees determined to hurt the company, but hardware, software and sensible security policies can protect proprietary data and internal communications from malicious outsiders.

Firewalls can be considered the first line of defense against LAN security breaches because they provide data confidentiality. Firewalls do not ensure data integrity or non-repudiation because they do not encrypt or authenticate data.

Desktop firewalls

Desktop firewalls are available for individual client workstations. Also known as personal firewalls, they offer protection for an individual system instead of an entire network. Tools such as Norton 360 (*www.symantec.com*), ZoneAlarm (*www.zonealarm.com*), McAfee Personal Firewall (*www.mcafee.com*) and Windows Firewall (included with Windows) can detect and respond to attacks on your computer system.

Desktop firewalls offer many firewall features, such as inspection of all incoming transmissions for security threats. When a firewall is used in conjunction with anti-virus software, a personal computer is very secure, provided that the user updates the anti-virus and desktop firewall software frequently.

Native desktop firewall software

NOTE:
You will explore your Windows 7 desktop firewall settings in Lab 8-6.

Increasingly, operating system vendors are providing native desktop firewall software. For example, Windows 7 includes a native desktop firewall that is enabled by default. You can customize your desktop firewall settings.

UNIX and Linux systems often provide applications that allow you to block connections, such as the following examples:

- **iptables** — found on newer UNIX and Linux systems
- **ipchains** — found on older UNIX and Linux systems

Desktop firewall features

Some desktop firewalls include the following features:

- **Logging** — You can determine when a connection was made, as well as its source. You can also discover the protocol and/or port that a remote user used to make the connection.

Internet Control Messaging Protocol (ICMP)
A subset of Internet Protocol that is most often used to determine whether a computer can communicate with the rest of the network.

- **Blocking protocols** — You can block various protocols, including Transmission Control Protocol (TCP), User Datagram Protocol (UDP), **Internet Control Messaging Protocol (ICMP)** and Internet Protocol (IP). If blocking TCP and UDP, you can select any port to allow or disallow. ICMP is an especially common protocol to block, because attackers often use it to flood network connections. However, blocking this protocol may cause problems when troubleshooting your computer's connectivity to the network, because ICMP is most often used to test whether a system is able to communicate on a network.

Default desktop firewall stances

Desktop firewalls can be configured in one of the following ways:

- **Default open** — allows all traffic except that which is explicitly forbidden
- **Default closed** — denies all traffic except that which is explicitly allowed

Blocking incoming and outgoing traffic

NOTE:
A network firewall may also block transmissions between a computer and the Internet.

Desktop firewalls can also be configured to block incoming and outgoing traffic. Most desktop firewalls block incoming traffic (for example, traffic from the Internet to your computer). Most desktop firewalls can also be configured to block traffic from your computer to computers on the network. If you are experiencing connection difficulties specific to one protocol on your local network, consider that a desktop firewall might be blocking transmissions.

CIW Online Resources – Online Exercise

Visit CIW Online at *http://education.Certification-Partners.com/CIW* to complete an interactive exercise that will reinforce what you have learned about this topic.

Exercise 8-7: Features of firewalls

In the following lab, you will explore options to consider when enabling a desktop firewall. Suppose you are the security administrator for a bank. The bank manager has asked you to protect employees' computers by restricting access to Internet resources. How would you configure the desktop firewalls to offer appropriate protection but still allow employee access to relevant Internet resources?

Lab 8-6: Viewing your desktop firewall settings

In this lab, you will view your Windows firewall settings.

1. Click **Start | Control Panel | System and Security | Windows Firewall** to display the Windows Firewall window, shown in Figure 8-13. Notice that the firewall is enabled by default, unless another firewall is present (e.g., a firewall packaged with anti-virus software). It can be turned on or off in the left-hand pane.

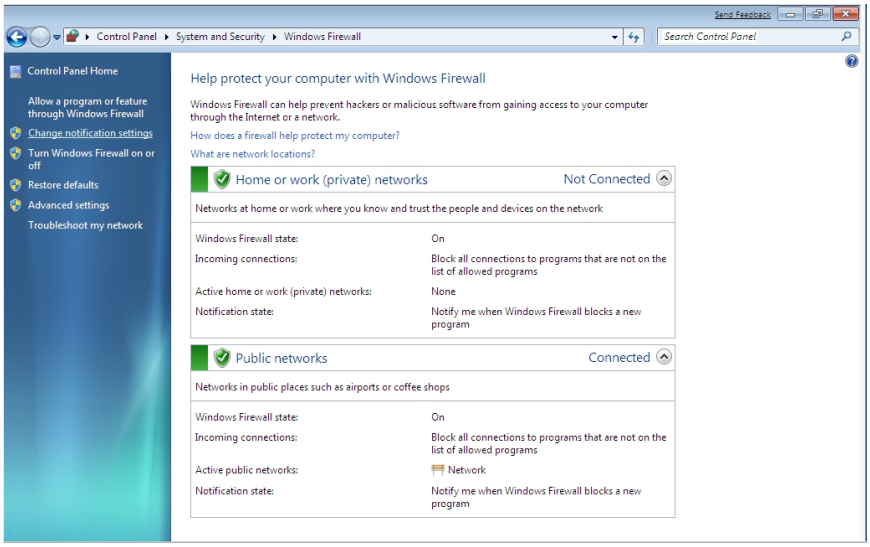

Figure 8-13: Windows Firewall window

2. Click the **Change Notification Settings** link in the left-hand pane to display the Customize Settings windows for Windows Firewall Settings. This window reconfirms that your desktop firewall is enabled. Notice the Block All Incoming Connections, Including Those In The List of Allowed Programs check box. You can select this option to block all programs from communicating with your computer in the event that you log in to an unsecure public Wi-Fi network. Click **OK**.

3. Click the **Allow a Program or Feature Through Windows Firewall** link in the left-hand pane. The selected items in the Allow Programs And Features list will be allowed to communicate through the desktop firewall. Unselected items will not be allowed to communicate through the firewall. You can select or deselect items as necessary, and you can add additional programs or ports that are not currently on the list. Your list should resemble Figure 8-14. Click **OK** when finished.

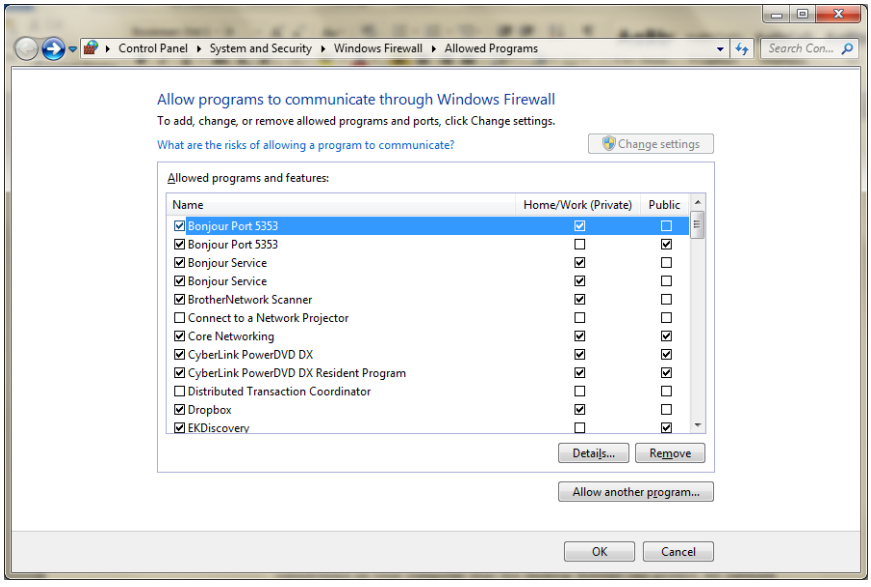

Figure 8-14: Windows Firewall Settings dialog box — allowed programs list

4. Click the **Advanced Settings** link. This window shows the available network connections on your computer that the desktop firewall can protect. All network connections are protected by default, but you have the option of disabling them if you want.

5. Close **Windows Firewall** without changing any firewall settings.

Security-Related Ethical and Legal Issues

The main function of IT professionals in any organization is to provide network and Internet-related services, and to protect system resources from unauthorized entry, malicious attackers and malware. IT professionals are also faced with ethical and legal issues related to the security of network and individual computer use by employees. In addition, the Internet has brought about new challenges to copyright, trademark and licensing law enforcement. Because the Internet spans numerous countries and each government has its own set of rules, new enforcement techniques must be applied. This section discusses privacy concerns, copyright issues, licensing issues, trademark issues and encryption policies.

OBJECTIVE
1.14.4: Copyright issues

Copyright issues

As you learned earlier in this course, copyright laws protect original works of authorship that are fixed in a tangible medium of expression. According to copyright law, the basic elements of authorship are:

- Expression.
- Originality.

An Internet user who uses an unauthorized copy of someone else's work is violating the copyright owner's rights. Remember that although copying text or images from a Web site is easy, the ability to do so does not make it legal to use someone else's work for your own purposes. Copyright infringement is a punishable crime.

If you or your company holds a copyright on your Web site material, you should place the copyright symbol (©) and year at the bottom of each page that contains the copyrighted material. Copyright symbols are not required but are highly recommended because they are often the first line of defense against copyright infringement.

International copyright?

Contrary to popular belief, an international copyright does not exist. To protect your copyright of your original material, you must contact the government agency that handles copyrights in the country in which you reside. For instance, in the United States, you would contact the United States Copyright Office. You can request the forms (depending on your specific work) by phone or download forms at *www.copyright.gov*. In Canada, you would contact the Canadian Intellectual Property Office (*www.cipo.ic.gc.ca*).

Information Infrastructure Task Force (IITF)

The Information Infrastructure Task Force (IITF) was formed in 1993 to codify copyright law as it applies to digital information. The IITF in turn established the Working Group On Intellectual Property Rights to examine the intellectual property implications of combining the existing infrastructures of radio, television, telephones, fax machines and computers into one information infrastructure of all communication mediums. The group's mission was to make recommendations for changes to U.S. intellectual property law and policy.

In 1994, the Working Group On Intellectual Property Rights published the "Green Paper," a preliminary report on intellectual property rights. The group recognized the need to review current copyright laws in light of the fact that copying and disseminating information is extremely easy in the digital age.

World Intellectual Property Organization (WIPO)

The World Intellectual Property Organization (WIPO) is a specialized United Nations agency formed to protect intellectual property worldwide. Intellectual property consists of industrial property (trademarks, inventions) and copyrighted works. WIPO attempts to enforce copyright laws through cooperation among countries. Ninety percent of the world's countries are members of WIPO.

If you register a copyright for a book in the United States, and someone reproduces and sells it in Germany without your permission, you would be able to prosecute that person in both the United States and Germany because both countries have signed copyright agreement documentation. The WIPO site (*www.wipo.int*) lists the copyright administration office for each member country.

Precedent copyright law and Internet cases

The following court cases and piracy violations have precedent-setting implications with respect to copyright laws and the Internet.

- **Sega Enterprises Ltd. vs. MAPHIA** — In *Sega Enterprises Ltd. vs. MAPHIA,* Sega Enterprises brought suit against MAPHIA, an electronic bulletin board system (BBS). Sega Enterprises claimed that MAPHIA copied Sega games to its BBS and made them available for user downloads. The court found that MAPHIA sometimes charged users a direct fee for downloading privileges, or bartered for the privilege of downloading the Sega games. Because Sega's games are protected by copyright, MAPHIA violated Sega's copyright by obtaining unauthorized copies of Sega's games and placing them on storage media of the BBS to be downloaded by unknown users. The courts found in favor of Sega Enterprises.
- **Playboy Enterprises vs. Frena** — In *Playboy Enterprises vs. Frena*, Playboy brought a lawsuit against the defendant George Frena, an independent BBS operator. Playboy claimed that Frena distributed unauthorized copies of Playboy's copyright-protected photographs from his BBS. Frena's BBS was available to anyone for a fee. Frena admitted that he did not obtain authorization from Playboy to copy or distribute the photographs. The courts found evidence of direct copyright infringement, and stated that the fact that Frena may not have known he was committing copyright infringement was irrelevant.
- **Recording Industry Association of America (RIAA) vs. Napster** — This copyright-infringement case was filed by the RIAA to contest the distribution of copyrighted music files over the Internet using a popular program called Napster. As you have learned, Napster allowed users who had installed the Napster software on their computers to share MP3 music files with other users who had the Napster software. No fee was charged for copying files from one user's computer to another. The RIAA wants artists and record companies to receive royalty payments from users who swap copyrighted files. Napster argued that because the MP3 files were transferred from user to user and were never in Napster's possession, Napster did not act illegally. The courts ruled in favor of the RIAA and required Napster to halt its services. Napster (*www.napster.com*) is still operating but now charges a per-track or per-album fee. Record companies such as Bertelsmann Music Group (BMG) have since joined with technology developers to create subscription services that will allow users to share

copyrighted MP3 files while observing a permission agreement. These arrangements allow artists and record companies to receive payment for their copyrighted music.

NOTE: Research the current status of the Megaupload.com case. Did the US have the right to shut down the site and arrest the owners?

- **United States vs. Megaupload.com** — Although this case may never go to court, it is an excellent example of copyright infringement. Megaupload was a hosting service established in Hong Kong that offered online storage and sharing of files, audio and video. On Jan. 19, 2012, the United States Department of Justice shut down their Web sites and seized the company's domain names. The owners were arrested for dedicating their business to copyright infringement. The Megaupload.com Web site displayed the warning shown in Figure 8-15 after the seizure.

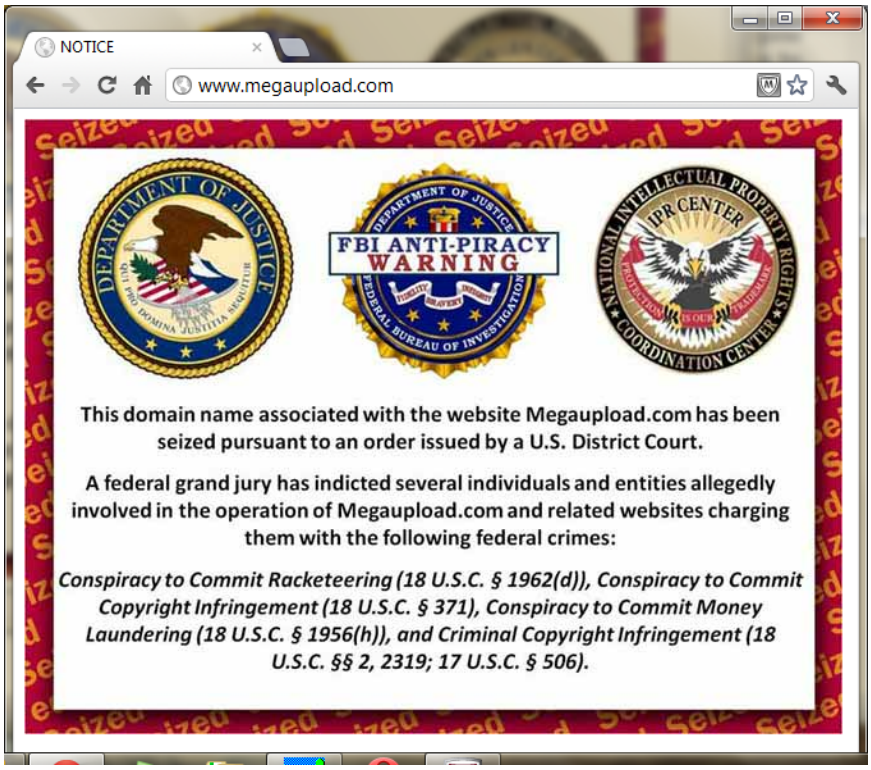

Figure 8-15: Megaupload.com shut down due to copyright infringement

Licensing issues

If you want to license someone else's copyright-protected material, you must contact the copyright owner and ask for permission. This task might involve contacting the legal department of a large organization, a copyright specialist at a small to midsize organization, or even an individual.

If you are granted permission to use copyrighted work, the copyright holder dictates the terms of use. For example, there may be no cost but you may be required to cite credit to the owner for the work. In most cases, you must license the work from the owner under the terms of an agreement. The agreement usually determines the way the work may be used (limited or unlimited reproduction) and the payment arrangement (attribution, royalties, lump-sum payment).

Trademark issues

A trademark is any word, slogan, symbol, name, package design or device (or any combination thereof) that marks and distinguishes a product from other products in

trade. For instance, Google and Acura are both trademarks. Trademarks are protected worldwide by participating WIPO countries.

To register a trademark, you must contact the government agency in your country that handles trademarks. For example, in the United States, you would contact the U.S. Patent And Trademark Office. You can request the forms by phone or download forms online from *www.uspto.gov*. In Canada, you would contact the Canadian Intellectual Property Office at *www.cipo.ic.gc.ca*.

CIW Online Resources – Course Mastery

Visit CIW Online at *http://education.Certification-Partners.com/CIW* to take the Course Mastery review of this lesson or lesson segment.

IBA Lesson 8 - Part B

Case Study

Legal Protection

Roberto is the network administrator for an international law firm with offices and customers in North America, South America, Africa and the Middle East. The lawyers frequently contact each other via e-mail, use the Internet to research cases, and use listserve groups to discuss recent cases and developments in international law.

Roberto wants to protect the company's network from malicious invasions, and limit the lawyers' access to the Internet and newsgroups. So he performs the following tasks:

- He ensures that firewalls are in place to prevent outsiders from accessing proprietary data on the law firm's private network, and to prevent internal users from accessing specific Internet resources.
- He installs anti-virus software on all computers and prepares a maintenance schedule to periodically update the software with the most recent virus signature profiles.
- He assigns user names and passwords that the lawyers must use to access the network.
- He configures Web browsers and e-mail clients to reject incoming file attachments that do not have digital signatures or digital certificates.
- He educates the lawyers on the steps they can take to prevent malware infection.
- He establishes encryption policies for sending sensitive information via e-mail.

* * *

As a class, discuss this scenario and answer the following questions:

- What other ways can Roberto protect the law firm's network resources from outside attack?
- Which protective measures do you consider too restrictive? Why?

Lesson Summary

Application project

Some computer viruses have received worldwide attention because of the damage they have inflicted. The PE_Nimda.A-O and the infamous W97M.Melissa.A worms spread globally because they were contained in executable e-mail and newsgroup article attachments. Stuxnet, Duqu, and Flamer made headlines because they demonstrate that war has moved from tanks and planes to the Internet via cyber-warfare.

Access the Symantec Security Response page at *www.symantec.com/security_response/index.jsp* or the Trend Micro Security Information page at *www.trendmicro.com/vinfo,* and research the PE_Nimda.A-O, W97M.Melissa.A, Stuxnet, or Duqu worms, or a more recent virus or malware toolkit. For each virus, identify precautionary measures that you can take to prevent your company's network from becoming infected.

Skills review

In this lesson, you learned techniques for protecting yourself online. "The Right to Be Forgotten" was discussed, along with the dangers of posting too much personal information on the Internet. You studied the way user names and passwords, as well as digital certificates and firewalls, can provide Web security and ensure secure online transactions. You learned about viruses, worms, trojans, illicit servers and spyware, and you studied methods you can employ to protect computers and networks from the harmful effects of viruses. You also learned about the privacy concerns, copyright issues, licensing issues and trademark issues facing IT professionals, as well as the need to encrypt company transmissions and establish company encryption policies. Finally, you learned about typosquatting and how it takes advantage of typographical errors that users make when inputting addresses into browsers.

Now that you have completed this lesson, you should be able to:

- ✓ 1.5.5: Define the function of Secure Sockets Layer (SSL), Transport Layer Security (TLS) and other encryption methods in securing communication for various protocols (e.g., FTP/FTPS, HTTP/HTTPS, IMAP/IMAPS, POP3/POP3S).
- ✓ 1.9.2: Identify advantages and disadvantages of using cookies, and set cookies, including setting a cookie without user knowledge, automatically accepting cookies versus query, remembering user actions, security and privacy implications.
- ✓ 1.10.1: Define the three major types of encryption.
- ✓ 1.10.2: Identify ways that authentication, digital certificates, encryption and firewalls provide Web security.
- ✓ 1.10.3: Identify ways that encryption helps enforce data confidentiality, data integrity and non-repudiation to secure end-user transactions.
- ✓ 1.10.4: Describe a computer virus and explain how to protect your computer from virus attacks.
- ✓ 1.10.5: Explain the functions of patches and updates to client software and associated problems, including desktop security, virus protection, encryption levels, Web browsers, e-mail clients.

- ✓ 1.10.6: Identify steps to take when you receive an unexpected attachment (e.g., via an e-mail or instant message client).
- ✓ 1.10.7: Identify steps to take when an attack is suspected.
- ✓ 1.10.9: Lock a computer to increase workplace security.
- ✓ 1.10.10: Distinguish between a virus and a worm.
- ✓ 1.10.11: Demonstrate the functionality of spyware.
- ✓ 1.10.12: Define the practice of typosquatting.
- ✓ 1.14.1: Define privacy concerns.
- ✓ 1.14.2: Identify appropriate use of company and personal systems.
- ✓ 1.14.3: Summarize personal privacy expectations versus an organization's right to know how its provided services are being used.
- ✓ 1.14.4: Identify basic copyright issues.
- ✓ 1.14.5: Explain the purpose of encrypting company transmissions and establish company encryption policies.
- ✓ 1.14.6: Discuss "The Right to Be Forgotten" and the possible ramifications of damaging posts on the Internet.

CIW Practice Exams

Visit CIW Online at *http://education.Certification-Partners.com/CIW* to take the Practice Exams assessment covering the objectives in this lesson.

IBA Objective 1.05 Review

IBA Objective 1.09 Review

IBA Objective 1.10 Review

IBA Objective 1.14 Review

Note that some objectives may be only partially covered in this lesson.

Lesson 8 Review

1. What is the difference between symmetric encryption and asymmetric encryption?

2. What is a digital certificate?

3. What is a firewall?

4. What is the difference between a virus and a worm?

5. What is the difference between malware and spyware?

6. What is the difference between a patch and an update?

