






Lesson 2

Protecting Your Computer

Lesson Contents

	Guidelines for Protecting Your Computer
	Best Practices for Securing Online and Network Transactions
	Measures for Securing E-Mail and Instant Messaging
	Measures for Protecting Your Computer
	Self Test

Lesson Introduction

You need to provide your identification to access your bank locker or your safe deposit box. This identification is to ensure that no one else is able to access your items.

Similarly, you can implement various security measures to minimize the threat to your computer and the data on it. This lesson introduces you to some common best practices that will help you to protect your operating system, software, and data on your computer.




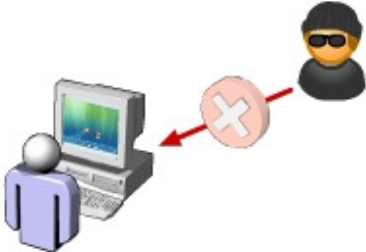

Lesson Objectives



After completing this lesson, you will be able to:

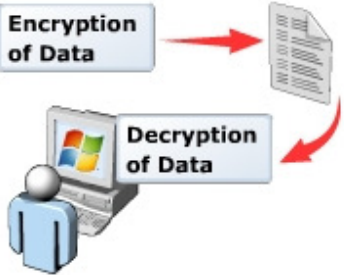
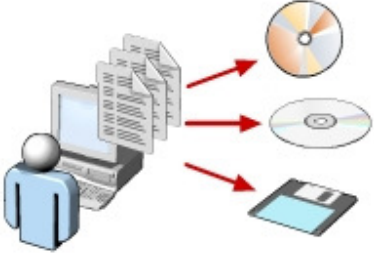
- Identify guidelines for protecting your computer.
- Identify best practices for securing online and network transactions.
- Identify measures for securing e-mail and instant messaging transactions.

Topic: Guidelines for Protecting Your Computer

Imagine that you have saved a confidential project report on your computer. You have been working for weeks to prepare this report and now you want to share the project report with your supervisor. You have a single copy of this report on your computer and it is important to secure the report from being tampered with or deleted. However, another employee uses your computer in your absence and deletes the project report from your computer. To avoid such situations, you can take measures to secure the data on your computer. The following table explains the actions that you can take to safeguard the operating environment and data on your computer.



Guideline	Description	
<p>Implement user identification</p>	<p>An effective way to minimize the risk to your operating environment and data is to keep unauthorized individuals from accessing your computer. One way to achieve this is by setting up accounts for authorized users of the computer, on the basis of which each user gets an appropriate level of access.</p> <p>For example, in Windows Vista, you can set up user accounts for each member of your family or other users. You can decide to give yourself more privileges, or in the case of a child's account, you can restrict the account's capabilities.</p>	 <p>The illustration shows a central Windows Vista logo with a computer monitor. Surrounding it are four circular icons, each representing a different user profile with a unique color and name. The profiles are blue, green, pink, and light blue.</p>
<p>Set username and password</p>	<p>You can also increase security and limit unauthorized access to your computer by setting up a username and password. In most offices, each employee has a unique username and password. The employees must provide the correct username and password to access their computers. You can set up users and passwords in Windows Vista.</p>	 <p>The illustration shows a person sitting at a computer. A red arrow points from the person towards a computer monitor. A red circle with a white 'X' is placed over the arrow, indicating a blocked or denied access. In the background, there is a silhouette of a person wearing a black hood and sunglasses, representing an unauthorized user or hacker.</p>
<p>Keep password secure</p>	<p>Your password acts like a key to your computer. Anyone who knows your password can access your computer and tamper with data. You must keep your password secure.</p> <p>Be careful while typing your password to prevent anyone else from seeing it. Do not share your password with others. Do not write the password and leave it on your computer or desk. If you think that the password has been compromised, change it immediately, before anyone else is</p>	 <p>The illustration shows a person at a computer. A yellow envelope icon with a red 'X' is shown next to the computer, representing a password that has been compromised or is being shared. To the right, there is a gold padlock icon, symbolizing security or a locked state.</p>



	able to misuse it.	
Lock computer	<p>When you leave your computer on and unattended, someone can tamper with your computer software or data. You can prevent this by temporarily locking your computer while you are away. When a computer is locked, it immediately hides the content of the screen and does not allow any operation until the computer is unlocked with the correct username and password combination.</p> <p>The exact steps to lock your computer depend on the operating system you are using. For example, in Windows Vista, you can lock your computer by pressing CTRL+ALT+DEL, and then clicking the Lock this computer button. Note that this feature of locking the computers is not available in all operating systems.</p>	
Install and update protective software	<p>You need to continuously guard your computer against threats such as viruses and spyware. At times, the damage due to a virus is considerable and you may lose important data or need to reinstall the operating system and other software. You can protect your computer from viruses and spyware by installing antivirus and antispyware software. These protective software programs help you detect and remove viruses and spyware present in your computer. They also prevent new ones from infecting your computer.</p> <p>It is a good practice to install a firewall, which filters out the content that reaches your computer. Installing a firewall also protects against hackers by restricting access by other online users.</p> <p>As newer threats keep appearing, software companies regularly create updates that you can install on your computer. These updates make additions to the installed software or operating system in your computer to make it less vulnerable to security threats. Ensure that you regularly update the antivirus software so that it can detect the newest viruses.</p> <p>Windows Vista includes Windows Firewall to protect your computer against unauthorized access. In addition, Windows Defender is a built-in antispyware program that protects against pop-ups and other security threats.</p>	



<p>Encrypt data</p>	<p>Converting your data to an unreadable form to protect it from unauthorized access is called encryption. An authorized user can reconvert the encrypted data into a readable and usable form. This is called decryption. Various software products today include a way to encrypt data.</p> <p>In Windows Vista, encryption is transparent to the user who encrypts the file. That is, you do not have to manually decrypt the encrypted file before you can use it. You can open and change the file as you usually do.</p>	
<p>Back up data</p>	<p>You can also help protect your files from loss or damage by making copies of important files and storing them on a different storage media, such as CDs, DVDs, or floppy disks. This process is known as backing up data. You should keep the backups in secure locations, so that you can use the backup data in case the original data is damaged or deleted.</p>	


Topic: Best Practices for Securing Online and Network Transactions

Connecting your computer to the Internet introduces it to a world of information and entertainment. However, it also leaves your computer vulnerable to many online threats. For example, it becomes easier for viruses to transfer from an infected computer to your computer. You can reduce the risks to your computer from these online threats by using a combination of best practices such as creating strong passwords, encrypting data, and using antivirus software. The following table explains the various actions that you can take to secure online and network transactions.

Action	Description	
<p>Use strong passwords</p>	<p>A strong password is a complex password, which cannot be guessed easily. The password should consist of a combination of uppercase and lowercase letters, numbers, and special characters such as <i>ampersand</i> and <i>number</i> sign, and should not contain complete words or names.</p> <p>A strong password is your primary defense against security and privacy threats. Strong passwords must be created for:</p> <ul style="list-style-type: none"> • Local access to standalone computers • Access to networks • Access to Web sites that have sensitive information, such as personal or financial details • Access to any valuable data • Personal data stored on your computer 	
<p>Protect against hacking and spyware</p>	<p>While you are browsing the Internet, it is possible that a software program installed on your computer is transmitting your personal information to a hacker in another country. Such software programs are examples of spyware. These programs generally get installed on your computer without your knowledge and secretly transfers confidential data from your computer to the hackers. Sometimes, employers deliberately install spyware on the computers used by the employees to track the computing activities of the employees.</p> <p>Windows Vista includes a built-in antispymware program called Windows Defender, which helps prevent spyware from getting secretly installed on the computer.</p> <p>Make use of Internet service provider (ISP) support</p>	

	<p>for online security. The support can be in the form of antivirus and anti-spyware software. Some ISPs even provide firewall protection, e-mail virus screening, and spam protection.</p>	
<p>Clear browsing history periodically</p>	<p>The Web sites and Web pages that you visit while browsing the Internet are saved in your browser's <i>History</i>. Also, while you browse the Internet, a number of files are stored in the temporary memory of your computer. This temporary memory is known as <i>cache memory</i>. The files stored in the cache memory record information about the Web pages you visit.</p> <p>However, some of these temporary Internet files may contain your personal information, such as your username and password, which can be accessed by hackers. To prevent hackers from accessing your personal information, regularly delete the contents present in the browser history and in the cache memory.</p> <p>While visiting a Web site, you may notice that it displays your name. This is made possible through the use of cookies. <i>Cookies</i> are small files that are created on your computer by previously visited Web sites to identify and track your preferences. Their purpose is to provide a more personal experience while visiting a Web site. However, cookies can also be a threat to computer privacy because they contain your personal information. For example, the cookies might contain your credit card details that you have used while shopping online. For these reasons, it is a good practice to periodically delete cookies to prevent your personal information from being misused.</p>	
<p>Avoid sharing personal information</p>	<p>Some Web sites require you to fill out forms containing personal information such as your name, gender, and age. In case of e-commerce sites, you might even need to share your bank account details or credit card number. But, remember that hackers can access and misuse this information. Some companies may also use this information to send you unwanted commercial e-mail messages. Therefore, before you share any personal information on a Web site, ensure that it is a secured Web site and there is a specific need to provide the information.</p>	

<p>Perform online transactions only on secure sites</p>	<p>While shopping online, you usually need to provide sensitive information such as your bank account number or credit card details. Therefore, it is important to ensure that you carry out online transactions only on secure Web sites. A Web site is secure if its name has the prefix <i>https</i>. The prefix indicates that the Web site implements the <i>Secure Sockets Layer (SSL)</i> protocol. SSL is an Internet security protocol that ensures secure data communication by encrypting the information transmitted. The SSL protocol certifies that the Web site is genuine and ensures that the data you provide to the site is not misused.</p> <p>When you enter a secure Web site, most of the Web browsers display a message to confirm that you have entered a secure Web site. The locked padlock icon that appears in the Address bar helps you identify a secure Web site. You can also check the security certificate of a Web site before performing any online transaction on that site.</p>	
<p>Configure security components by using Windows Security Center</p>	<p>Windows Security Center is a feature in Windows Vista, which provides you a convenient utility to check the status of essential security settings and track the antivirus software installed on your computer. You can open Security Center from Control Panel. The Security Center has four components:</p> <ul style="list-style-type: none"> • <i>Firewall</i>. In Windows Vista, Windows Firewall is automatically activated. The firewall helps prevent malicious content, such as viruses and worms, from entering your computer. • <i>Automatic updating</i>. This feature checks for relevant security-related updates available on the Microsoft Update Web site. Enabling this feature ensures that your computer remains updated and protected against the newest security threats on the Internet. • <i>Malware protection</i>. Spyware and other potentially unwanted software can install itself on your computer without appropriately obtaining your consent. Windows Defender provides real-time protection against such software while you are connected to the Internet. • <i>Other security settings</i>. Other security settings include Internet settings and User Account Control settings. Using Internet options, you can set the security level to medium, medium-high, or high. Internet Explorer 7 has higher security levels than its previous versions. User Account Control 	

	<p>prevents unauthorized changes to your computer by asking for the password before making changes.</p>	
<p>Disable active content</p>	<p><i>Active content</i> refers to small programs that get installed on your computer while you are browsing the Internet. Their basic function is to provide you with an interactive Internet experience through videos and toolbars. However, in some cases, these programs can be used to damage the data stored on your computer or install malicious software without your consent. By using your browser settings, you can disable active content to prevent the installation of such programs.</p>	

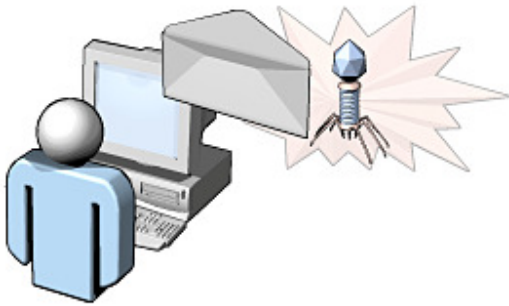
Topic: Measures for Securing E-Mail and Instant Messaging

E-mail and Instant Messaging (IM) are widely used for business and personal communication. However, hackers, online predators, and the people who create worms and viruses use e-mail and IM for malicious purposes. For example, these people can send e-mail attachments containing harmful software. These people can also use e-mail to solicit sensitive information or to lure you into fake offers. It is therefore important for you to take certain measures to ensure e-mail and IM security.

To ensure e-mail security, avoid opening e-mail with attachments, do not respond to junk mail, do not respond to unsolicited commercial mail, and protect yourself from phishing. To ensure IM security, chat with known people only and do not open attachments received over IM. The following table explains the actions to ensure e-mail and IM security.

The following table contains the transcript of an online animation.

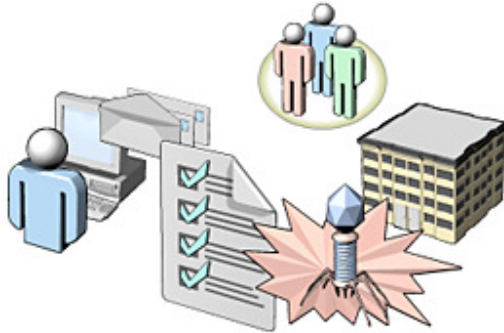
Be cautious when opening e-mail messages with attachments



You can send e-mail attachments to share files with your friends. You might receive a photograph or a music file as an attachment in an e-mail message. However, you need to be cautious while opening any mail containing an attachment because it is the most common pathway for the spread of viruses.

The following table contains the transcript of an online animation.

Do not respond to unsolicited commercial mail

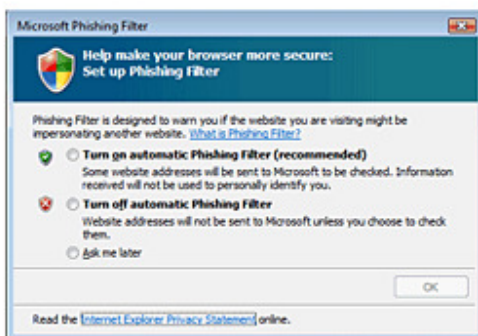


You may receive a number of unwanted e-mail messages from unknown senders including individuals and companies that are advertising their products or services. These messages may also be in the form of online surveys that require you to fill up personal information. These unsolicited messages are known as junk mail or spam.

Junk mail can often include content that is harmful for your computer. In addition, junk mail is often used for stealing identities, and you might accidentally share sensitive information while responding to such messages. Therefore, you should avoid replying to junk mail. You should also delete junk mail whenever you receive it. E-mail programs, such as Windows Mail, include a junk mail folder to which the junk mail may be directed and later deleted.

The following table contains the transcript of an online animation.

Protect yourself from phishing

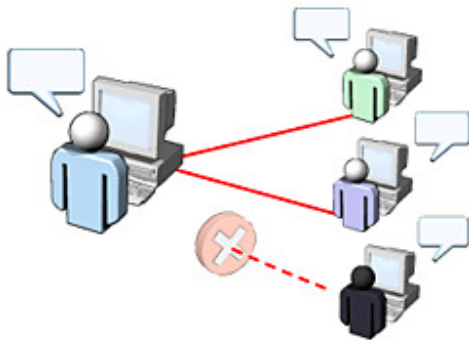


Phishing is a common activity used to extract personal information from computer users and then use the information for malicious purposes. For example, someone sends e-mail messages to you, pretending to be from a bank or any other trustworthy organization, and asks for sensitive information, such as credit card number or password. This information is either sold further or used to cause financial loss to you. Therefore, you must verify the authenticity of such e-mail messages before responding with any personal information.

Such e-mail messages are used by various phishing Web sites on the Internet to collect your personal information. Internet Explorer 7 includes the Microsoft Phishing Filter feature that runs in the background while you browse the Internet and helps detect phishing Web sites.

The following table contains the transcript of an online animation.

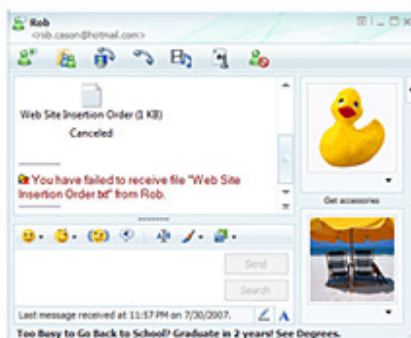
Limit chat activity to people whom you know



You should limit your chat activity only to the people whom you know. Developing communication with new and unknown individuals makes you more vulnerable to threats such as online predators and scams.

The following table contains the transcript of an online animation.

Avoid opening instant messenger attachments



Instant messaging is a common pathway for malicious attachments. You must avoid opening any attachments that you receive in an instant message, unless you are absolutely sure about its origin. An instant messaging attachment might contain a virus or spyware, which can harm your computer.

Topic: Measures for Protecting Your Computer

Sort the measures to protect your computer into their associated categories by writing the statement number in its corresponding option box.

Statement	
1	Clear browsing history periodically
2	Back up data
3	Avoid sharing personal information
4	Install and update protective software
5	Implement user identification
6	Protect against hacking and spyware
7	Keep password secure
8	Disable active content

Option 1		Option 2
Avoid Online Threats		Protect Computer Data

Note: The correct answers are shown on the next page.

Option 1		Option 2
Avoid Online Threats		Protect Computer Data
8, 6, 3, 1		7, 5, 4, 2

Question 1

One of the most effective ways to protect the software and data in your computer is to restrict the use of your computer to a defined set of individuals. Which of the following methods can you use for this purpose?

Select all answers that apply.

<input type="checkbox"/>	Update your operating system.
<input type="checkbox"/>	Set up user accounts.
<input type="checkbox"/>	Install antivirus software.
<input type="checkbox"/>	Keep passwords secure.

Question 2

Various types of files are created on your computer while using the Internet. Some of these might present a threat to security, but are actually present for the benefit of the user. Which of the following are examples of such files?

Select all answers that apply.

<input type="checkbox"/>	Cookie.
<input type="checkbox"/>	Virus.
<input type="checkbox"/>	Active Content files.
<input type="checkbox"/>	Worm.

Question 3

Which of the following methods will you use to secure your e-mail and IM transactions?

Select all answers that apply.

<input type="checkbox"/>	Delete e-mail messages from unknown senders without opening them.
<input type="checkbox"/>	Forward unsolicited e-mail messages to a friend for advice.
<input type="checkbox"/>	Reply with personal information to an e-mail message if the sender is a bank employee.
<input type="checkbox"/>	Avoid opening attachments received in instant messages.

Note: The correct answers are shown on the next page.

Answer 1

One of the most effective ways to protect the software and data in your computer is to restrict the use of your computer to a defined set of individuals. Which of the following methods can you use for this purpose?

Select all answers that apply.

Update your operating system.

Set up user accounts.

Install antivirus software.

Keep passwords secure.

Answer 2

Various types of files are created on your computer while using the Internet. Some of these might present a threat to security, but are actually present for the benefit of the user. Which of the following are examples of such files?

Select all answers that apply.

Cookie.

Virus.

Active Content files.

Worm.

Answer 3

Which of the following methods will you use to secure your e-mail and IM transactions?

Select all answers that apply.

Delete e-mail messages from unknown senders without opening them.

Forward unsolicited e-mail messages to a friend for advice.





Reply with personal information to an e-mail message if the sender is a bank employee.

Avoid opening attachments received in instant messages.

Lesson 3

Protecting Your Family from Security Threats

Lesson Contents

	Measures to Protect Your Privacy
	Online Predators
	Guidelines for Protection from Online Predators
	Self Test

Lesson Introduction

Computers are not only used at schools, colleges, and offices, but are also commonly used in homes. You use computers for various purposes such as to keep household accounts, exchange e-mail messages with family and friends, browse the Internet, and play games and music. Every member of your family can find some use for the computer.

With increase in the use of computers at home and at work, it is important that you and your family understand the various threats associated with the use of computers and the Internet. In this lesson, you will learn about the various measures that can help protect your computer from these threats.



Lesson Objectives

After completing this lesson, you will be able to:

- Identify measures that you can use to protect your privacy.
- Explain how online predators operate.
- Identify guidelines to protect your family from online predators.

With the growing popularity of computers and the Internet, there are multiple ways in which your privacy is compromised. You and your family members need to prevent these threats to privacy. You can take the following simple measures to safeguard yourself and your family members against invasion of privacy.

Shield Your Identity

Avoid sharing your personal information with anyone, unless you know the person. This is the golden rule of protecting privacy. While exchanging e-mail messages or chatting through instant messenger, ensure that you do not reveal personal details about you or others known to you. Also, use strong passwords for access to your computer and e-mail connections.

Make Regular Backups of Your Computer and Important Data

It is a good practice to back up all types of the important and sensitive data on your computer. Important data might be documents, databases, or contact information. You can use various storage media such as compact disc or another hard disk to back up your data. If you regularly back up the data stored on your computer, you can recover the data in case the original data is damaged or deleted. Also, it is advisable to store the backup data in a secure place and restrict access to it by using passwords and encryption.

Check Current Security of Your System Regularly

Check the current security level of your computer regularly. Modern operating systems have built-in features that help you track the ability of your computer to safeguard against various threats to security and privacy. For example, Windows Security Center is a component in Windows Vista, which helps you to maintain firewall settings, set up schedules for software updates, and check the validity of the antivirus software installed on your computer.

Run Virus Scans Daily

Each day when you access the Internet, there is a chance that your computer is infected by viruses. Therefore, it is important that you run a virus scan on your computer everyday. You also need to keep the antivirus software on your computer up-to-date to protect your computer from new viruses.

Use Antispyware

Spyware programs can secretly enter your computer and transmit personal information about you and your family. Use antispyware software to keep a check upon these malicious programs, and keep the software up-to-date.

Perform Online Transactions on Secure Web Sites with Reputable Vendors

When you perform an online transaction, you need to provide your personal information, such as your credit card details or bank account details, to the Web site. This information, if disclosed to others, can be misused for financial fraud. Therefore, it is important that you carry out online transactions only on secure Web sites.

Report Abuse to the ISP

Most reputable ISPs have a set of terms and conditions that does not allow its users to follow any unethical or illegal practices. You should report to the ISP whenever someone attempts to invade your online privacy by sending you spam or attempts to hack your computer. This allows the ISP to take action against such individuals.

Filter E-mail Messages from Unknown/Anonymous Senders

You may receive a number of e-mail messages from individuals unknown to you. Such e-mail messages, referred to as spam or junk mail, can often be carriers of viruses or spyware. Hackers attempting to retrieve your personal information can also send you junk mail. Therefore, it is important to be careful while dealing with them. With e-mail software programs, you can create e-mail filters that help you block the junk mail. You must also ensure never to respond to junk mail because it can lead to an increase in unwanted messages and accidental sharing of personal information.

Encrypt Sensitive E-mail Messages, If Possible

Using encryption is a simple and effective way to ensure that your e-mail communication remains confidential. Encryption is the process of encoding the e-mail message in such a manner that it appears unreadable to everyone except the intended reader. Most e-mail software, such as Windows Mail, provides this e-mail encryption feature.

Topic: Online Predators

The Internet is a popular medium of communication for people all over the world. You can get acquainted with someone while actually knowing very little about the identity and intentions of the individual. This aspect of the Internet communication can be misused by people to lure young individuals into inappropriate or dangerous relationships. The people who engage in such activities are known as online predators.

Online predators generally target children, especially adolescents. It is during adolescence that children gradually move out of parental control and look for new relationships. Online predators attempt to establish a relationship of trust and intimacy with these children. Online predators can also target adults with the objective of financial exploitation.

Online predators trap their victims by developing contact through chat rooms, instant messaging, e-mail, or discussion boards. Among the various tools, chat rooms are the ones most commonly used by these predators. Online predators often assume a fake identity as a member of a specific chat room. For example, if the chat room belongs only to children, an online predator can easily assume the identity of a child in order to participate in that chat room.



Topic: Guidelines for Protection from Online Predators

You and your family members can become the target of online predators. These predators may try to establish contact with you or your family members to exploit you financially. The predators may also try to involve you and your family members in inappropriate relationships. The following table lists some guidelines that you can follow to protect yourself and your family from online predators.

Guideline	Description
Know the signs of predator behavior	Online predators have some predictable behaviors, which can help you identify them easily. Online predators tend to get intimate very quickly. They often express a great deal of interest and affection toward their targets. You need to ensure that you and your family members can detect such behavior to avoid contact with potential online predators.
Be cautious of offers from strangers online	Online predators usually lure their targets with gifts or other tempting offers. You should be cautious about such gifts or offers. Also, educate your family members to be suspicious about gifts offered over the Internet.
Educate your family on online safety measures	<p>Educate your family members on appropriate chat room behavior to avoid being targeted by online predators. Tell them to use nonsuggestive and neutral screen names. The screen names must not give away their actual name, age, gender, or contact information because this information can be misused.</p> <p>Some Web sites try to extract information under the pretext of feedback or surveys. Tell your family not to reveal any personal information to these Web sites without your permission. Also, ensure that your family do not give out any personal details, such as name, last name, address, and phone number, in chat rooms and bulletin boards. Your family members must not share their username and password with anyone, including friends.</p>
Guide children when they visit Web sites	<p>As parents, restrict young children from visiting Web sites that are inappropriate for them, or those Web sites that bring them in contact with potential online predators. It is recommended that parents guide their young children when the children visit any Web site.</p> <p>As a parent, instruct your children to leave a Web site if it makes them uncomfortable or if the site contains any unpleasant content. Also, educate your children to leave a Web site that asks for excessive personal information.</p>
Know the sites visited by children	It is important for parents to regularly check the type of Web sites their children visit. You can track the previously visited Web sites by viewing the browser history or by using software that help you track the online activity of a computer.
Block access to inappropriate Web sites	You can enable your browser's Content Advisor feature to control the type of Web sites that your family members can visit while browsing the Internet. By using this feature, you can restrict children from visiting Web sites that contain

	adult content. You can also install certain software programs that help you block specific Web sites.
Monitor chat activities	Specialized software can monitor chat activities and flag inappropriate information exchange on your computer. You can install these software to track the chat activities of your children.

Topic: Self Test

Each pair of statements contains a true statement and a false statement. For each pair of statements, indicate which statement is true by placing a mark in the True column to the right.

	Statement	True	False
1	Replying to junk mail CAN cause you to reveal personal information.		
2	Replying to junk mail CANNOT cause you to reveal personal information.		
3	Online predators GET intimate very quickly.		
4	Online predators DO NOT GET intimate very quickly.		
5	SPYWARE software helps you keep a check on malicious programs.		
6	ANTISPYWARE software helps you keep a check on malicious programs.		
7	It is POSSIBLE to monitor chat activity.		
8	It is NOT POSSIBLE to monitor chat activity.		
9	Encryption COMPRESSES the e-mail message so that it appears unreadable.		
10	Encryption ENCODES the e-mail message so that it appears unreadable.		
11	Online predators DO NOT TARGET children.		
12	Online predators TARGET children.		
13	Children SHOULD be allowed to visit Web sites alone.		
14	Children SHOULD NOT be allowed to visit Web sites alone.		
15	Online predators DO NOT LURE their targets with gifts.		
16	Online predators LURE their targets with gifts.		
17	The screen name used for chatting SHOULD NOT be your real name.		
18	The screen name used for chatting SHOULD be your real name.		

Note: The correct answers are shown on the next page.

	Statement	True	False
1	Replying to junk mail CAN cause you to reveal personal information.	✓	
2	Replying to junk mail CANNOT cause you to reveal personal information.		✗
3	Online predators GET intimate very quickly.	✓	
4	Online predators DO NOT GET intimate very quickly.		✗
5	SPYWARE software helps you keep a check on malicious programs.		✗
6	ANTISPYWARE software helps you keep a check on malicious programs.	✓	
7	It is POSSIBLE to monitor chat activity.	✓	
8	It is NOT POSSIBLE to monitor chat activity.		✗
9	Encryption COMPRESSES the e-mail message so that it appears unreadable.		✗
10	Encryption ENCODES the e-mail message so that it appears unreadable.	✓	
11	Online predators DO NOT TARGET children.		✗
12	Online predators TARGET children.	✓	
13	Children SHOULD be allowed to visit Web sites alone.		✗
14	Children SHOULD NOT be allowed to visit Web sites alone.	✓	
15	Online predators DO NOT LURE their targets with gifts.		✗
16	Online predators LURE their targets with gifts.	✓	
17	The screen name used for chatting SHOULD NOT be your real name.	✓	
18	The screen name used for chatting SHOULD be your real name.		✗