Internet Security

Module 6

Simplifying Security.

Certified Secure Computer User

Module 6: Internet Security

Exam 112-12

Module Objective

Internet security involves basic security measures to protect a user's account from attacks when connected to the Internet. It explains **security elements** that are necessary for the user to use the Internet safely.

This module will familiarize you with:

- Internet Security
- Internet Explorer Security Settings
- Mozilla Firefox Security Settings
- Google Chrome Security Settings
- Apple Safari Security Settings
- Instant Messaging (IM)
- Searching the Web
- Online Gaming and MMORPG
- Online Gaming Risks
- Security Practices Specific to Gaming
- Child Online Safety
- Role of Internet in Child Pornography
- Protecting Children from Online Threats
- How to Report a Crime?
- Internet Security Checklists
- Internet Security Laws

Module Flow

Browser Security

Search Engine and IM Security

Online Games

Child Online Safety

Internet Security Laws

Internet Security

Internet security involves protecting the user's data and information from **unauthorized access** when connected to the Internet. It also includes the protection of personal computers from viruses, worms, malware, spyware, and other attacks such as identity theft. Ways to launch an attack on Internet include:

- **Emails**:

  Emails are an important means of **communication** over Internet. However, emails can be used to attack a system through email viruses and email spoofing. Email spoofing displays many fake sources instead of the genuine source. When the user opens the message, it spreads the virus into the user's system. These viruses enter the user's system and weaken its functionality, allowing the attacker to compromise the system. These viruses can also enter the systems through **attachments** when an attacker attaches the virus program to the email.

- **IM**:

  Instant messaging (IM) opens the door for **spreading malware**, worms, spyware, viruses, spam, and root kits that result in the loss of productivity and personal data. Some outbound threats involved in here are "holes" that leak and lead to the loss of personal data and privacy.

- **Chat Rooms**:

  Chat rooms provide ways to connect to the world. Online chat rooms are not totally safe, as attackers create **fake profiles** to cheat users. Users should not believe such fake profiles, which often employ gambits such as being friendly. Users should not dispose their personal details over chat rooms. Before giving personal details, users should double check their friends' profiles. In particular, users should not disclose their bank account details and personal transaction details to the chat room friends.

- **File Sharing and Downloads**:

  File sharing allows the user to share files, documents, and media with other users over the Internet. These files and downloads may **contain harmful viruses**, malware, and worms. Users should be wary of these files and downloads.

Internet Explorer Security Settings

Configure security settings in your browser to avoid threats such as viruses, malware, and worms.

Launch **Internet Explorer**, click the **Tools** button, and select **Internet Options.**

Select the **Security** tab, which classifies websites into four zones:

- Internet

- Local Intranet
- Trusted sites
- Restricted sites

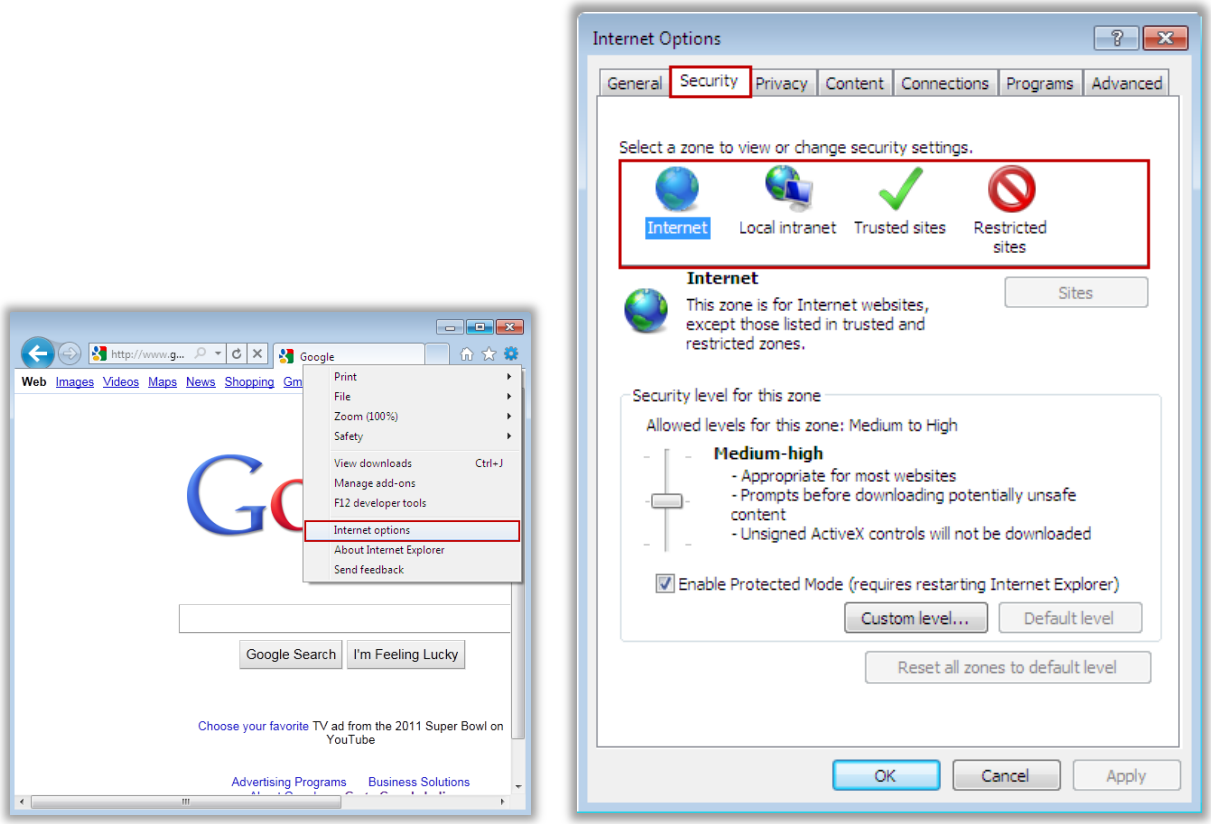

Figure 06-01: Windows Internet Explorer Options

Internet Explorer Security Settings: Internet Zone

The Internet Explorer includes predefined zones: Internet, Local Intranet, Trusted Sites, and Restricted Sites. A user can set the security options for each zone and add or remove websites from the zones by estimating the level of trust or risk in a particular website. The Internet zone is for all websites except those listed in the trusted or restricted zones.

- Click **Custom level…** to set the Internet zone security settings.
- Disable or enable the required options.
- Alternatively, move the slider to change the security level.
- Set the Security level for the zone to **High** to ensure higher security; however, maintaining a higher security level may degrade the performance of the browser.
- Click **OK** to apply the settings.

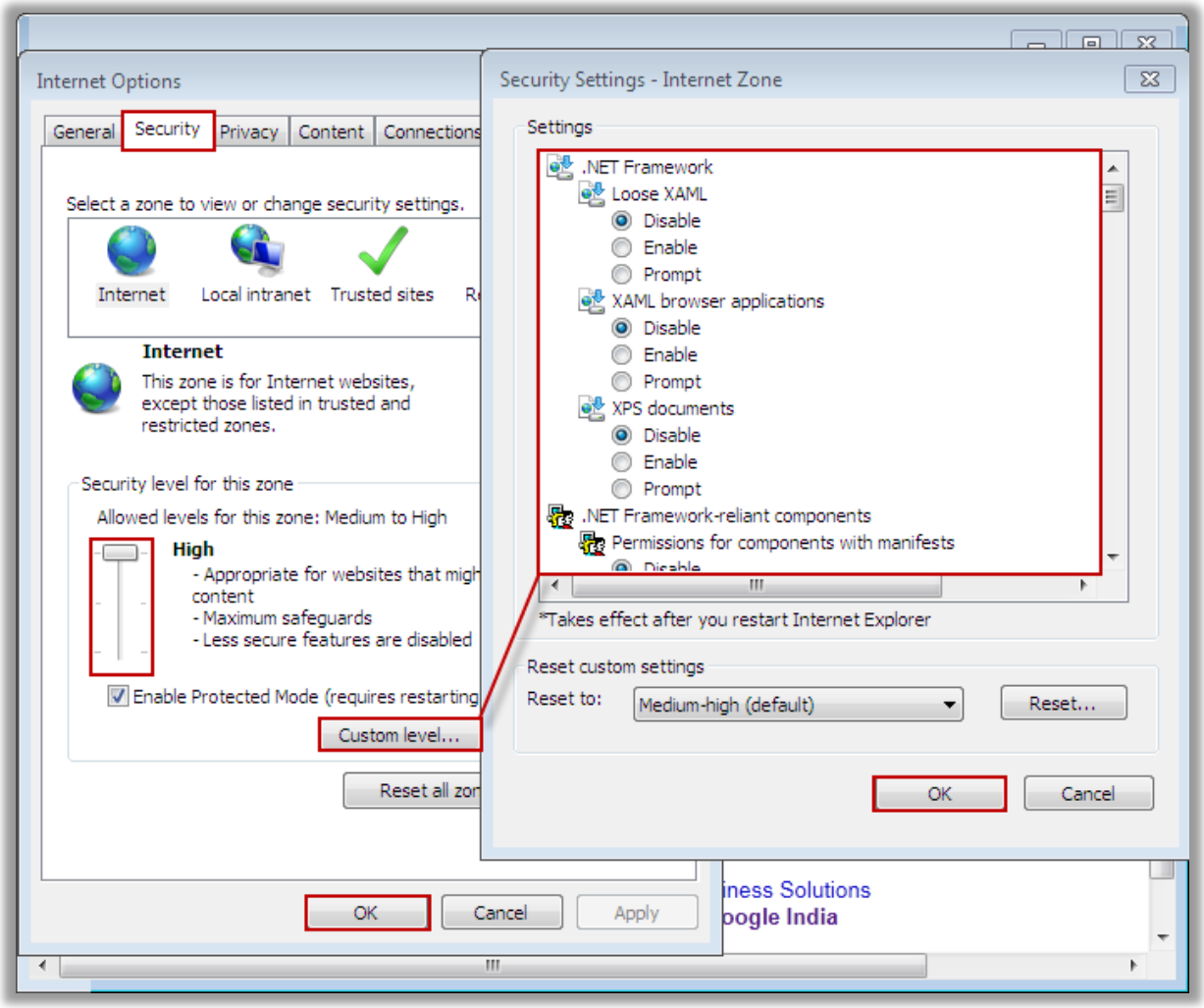

Figure 06-02: Windows Internet Options

Internet Explorer Security Settings: ActiveX Controls

ActiveX controls are the building blocks of a small program that distribute applications through the browser. They include customized applications that are required to gather data, view files, and view animation on websites. By default, Microsoft sets the security settings in Internet Explorer to **Medium** which allows the application to download and run **signed ActiveX controls**. However, if the user would like to change the Internet Explorer settings to high, low, or disable the prompting of ActiveX downloads, then they have to move the security level slider either up or down in the Internet Options' Security settings window.

Malware can be downloaded on a user's system through ActiveX controls when he or she visits some malicious websites. To protect systems from ActiveX threats:

- Disable the **ActiveX Controls and plug-ins** options in the **Security Settings** window.

- Enable the **Automatic prompting for ActiveX controls** option so that the browser prompts when an ActiveX control or plug-in needs to be enabled.
- Click **OK** to apply the settings.

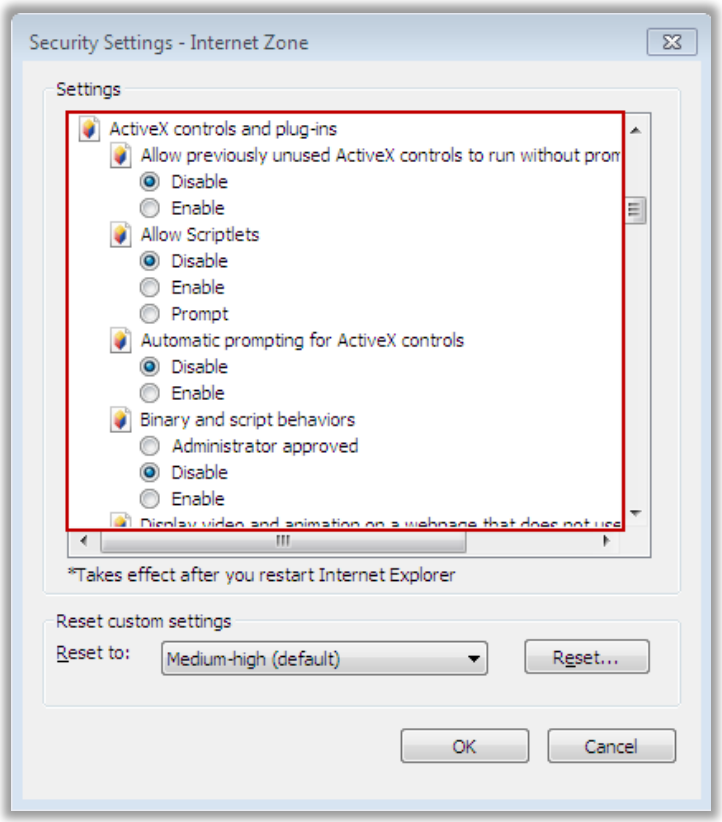

Figure 06-03: Window Security Settings

Internet Explorer Security Settings: Local Intranet Zone

The Local Intranet Zone covers the sites on Intranet. To add websites to the Local Intranet Zone:

- Select **Security →Local Intranet.**
- Click **Sites.**
- Click the **Advanced** button.
- Enter the URL into the **Add this website to the zone:** column and click **Add.**
- Click **OK** to apply the settings.

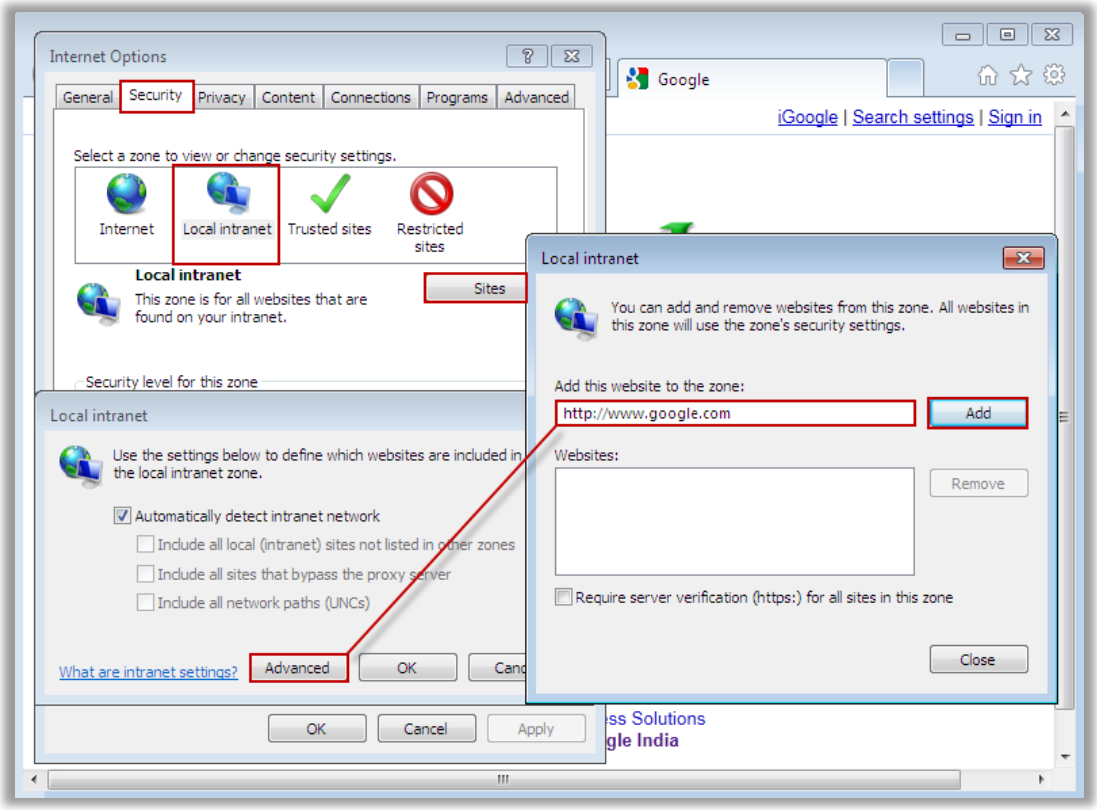

Figure 06-04: Windows Local Intranet Options

Internet Explorer Security Settings: Trusted Zone

A trusted zone contains those websites that a user believes will not damage his or her computers or data.

To add websites to the trusted sites zone:

- Select **Security** → **Trusted** sites.
- Click the **Sites** button.
- Enter the URL into the **Add this website to the zone:** column and click **Add.**
- Click **OK** to apply the settings.

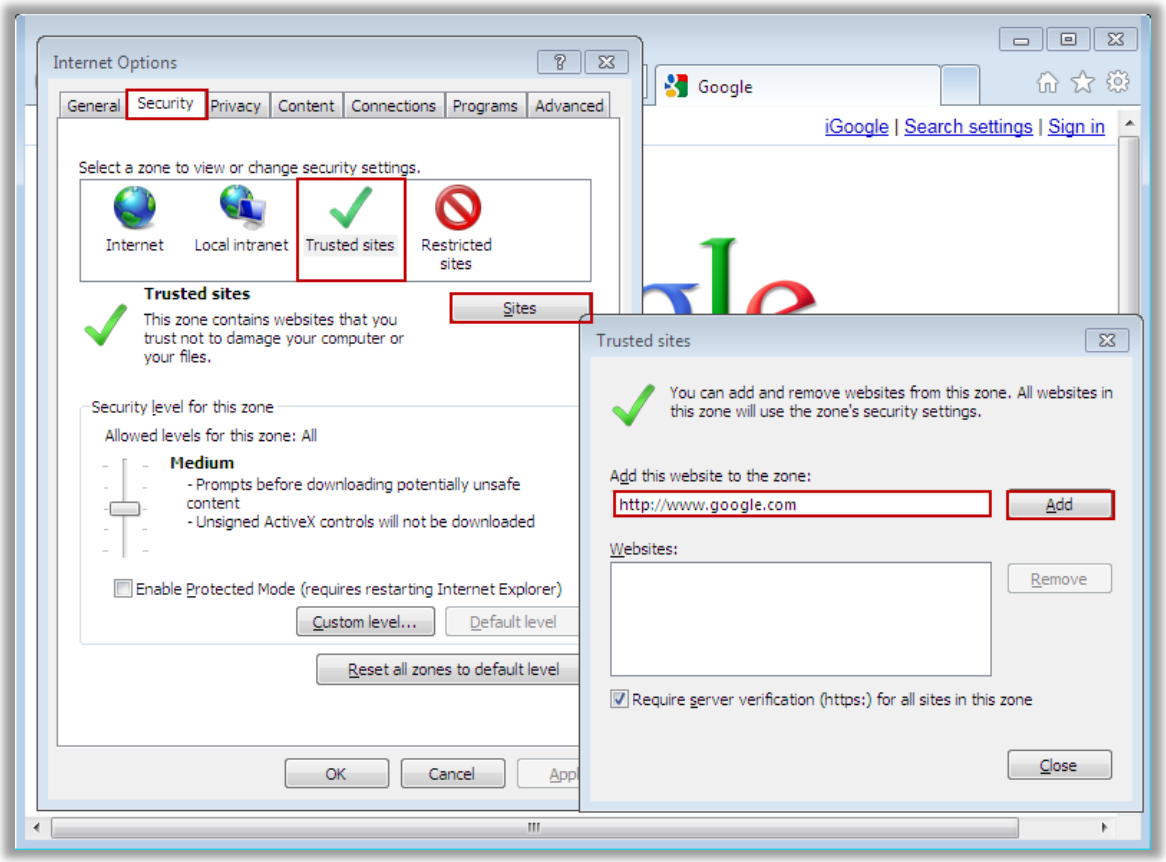

Figure 06-05: Windows Trusted Zone Options

Internet Explorer Security Settings: Restricted Zone

The restricted zone restricts access to the websites that might damage a computer. Users can **avoid accessing** a restricted site by adding it to the restricted zone. The Restricted Sites zone will help prevent the installation of unwanted applications, reduce unwanted pop-ups, and not allow sites to run unwanted scripts. This setting also protects the privacy by not sending cookies to sites in the Restricted Sites zone.

To add restricted websites to the restricted zone:

- Select the **Security** tab and choose **Restricted sites.**
- Click the **Sites** button.
- Enter the site URL into the **Add this website to the zone:** column to restrict the access.
- Click **Add** and then **OK** to apply the settings.

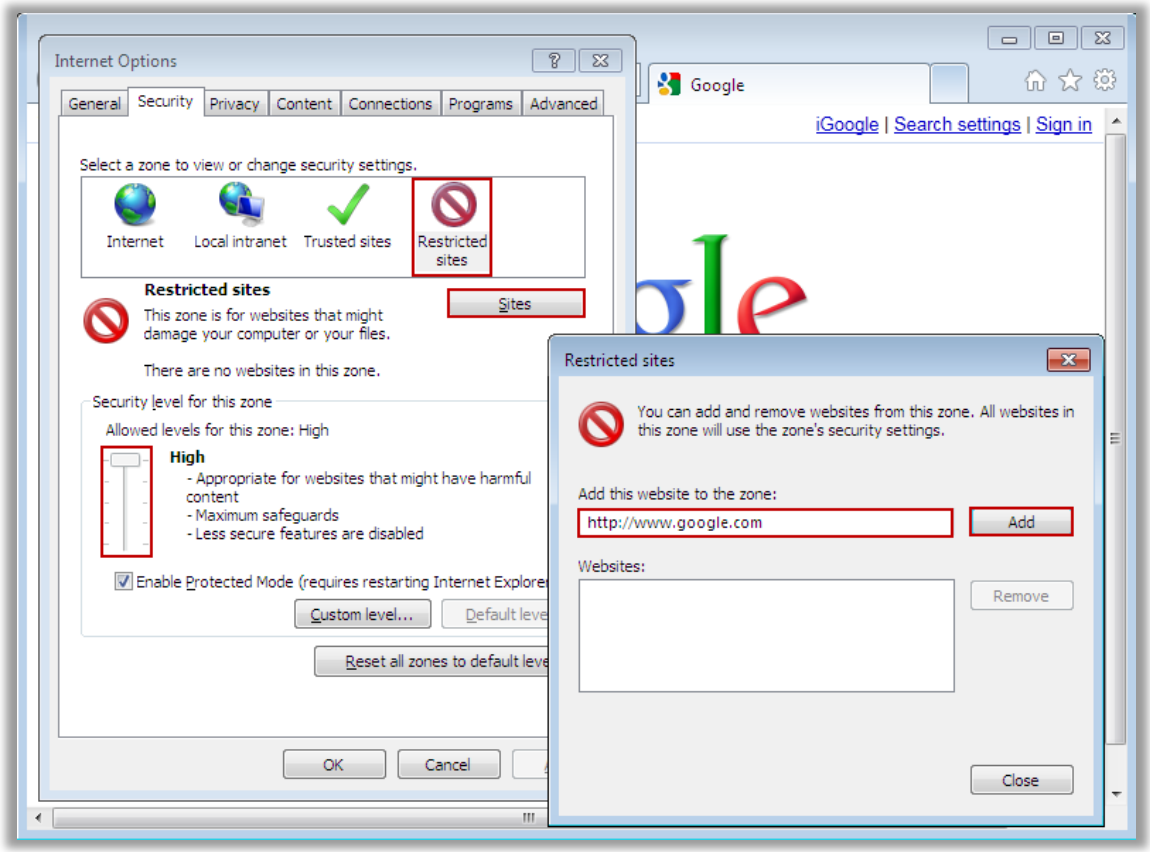

Figure 06-06: Windows Restricted Zone Options

Understanding Cookies

A cookie is information provided by a web server to a web browser and then sent back unchanged by the browser each time it accesses that server.

- When the website is revisited, the browser **sends the information back** to the server to help recognize the user.
- This activity is **invisible** to the user, and is generally intended to improve the web surfing experience (e.g., at an online store).
- It is used to remember information about a user, such as **session tracking** and usernames, and it is also used to authenticate the user.
- Cookies are not viruses or malware, but they can track users. For this reason, many antivirus programs detect cookies as malware.

Internet Explorer Privacy Settings

Information stored in a cookie is limited to whatever the user volunteers, such as when filling out a form on a webpage to request information or to make an online purchase. It is only a text file and cannot search a drive for information or carry a virus.

- To configure cookie settings:
  - Choose **Internet Options** from the **Tools** menu on the browser.
  - Select the **Privacy** tab and use the slider to set the level at low, medium, medium-high, or high.
  - **Block** all or **accept** all cookies, depending on the requirement.
  - Check the **Turn on Pop-up Blocker** option to block pop-ups that appear while visiting websites.

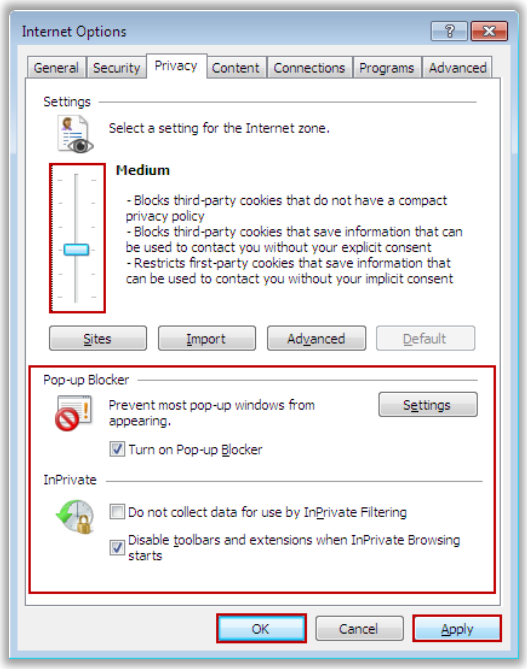

Figure 06-07: Internet Explorer Privacy Settings

Delete Browsing History

To save your computer's hard disk space and to keep the Internet **browsing private**, it is necessary to delete your Internet History. Always delete browser history because it can reveal your Internet activity to others.

- Choose **Internet Options** from the **Tools** menu on the browser.
- Go to the **Browsing history** section.

- Check the desired options in **Delete Browsing History** window**.**
- Click **Delete** to delete browsing history.

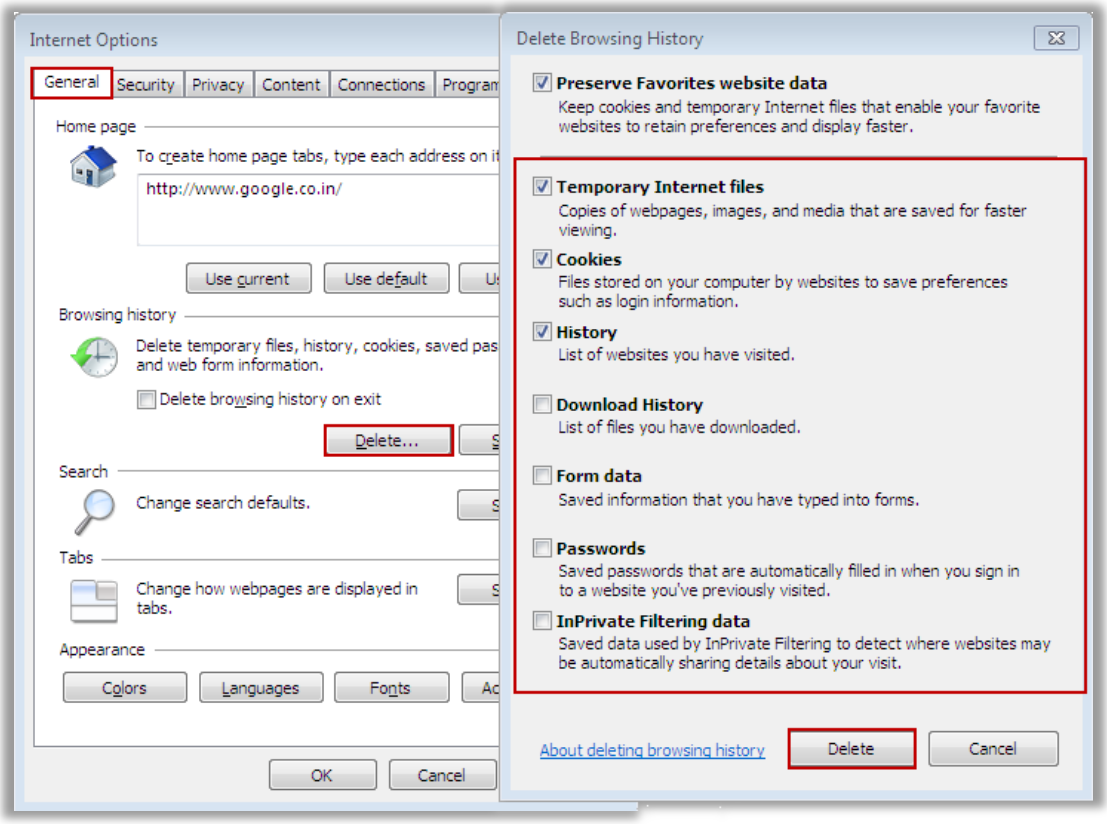

Figure 06-08: Deleting Browsing History Option Window

Do Not Allow the Browser to Remember any Password

When a user visits a websites for the first time that asks for a password, the system browser asks you "if you want it to **remember the password**.

All the browsers have this facility to save password and the user don't have to remember different passwords that he/she has created for different sites.

But this feature can pose **serious threats** to the user. If the system is infected with some advanced threats like viruses which tend to look for stored passwords and send them to malware servers managed by attackers. The best remedy to combat this kind of threats is to never allow the Internet browser (or any security program) to save passwords for you by not checking/unchecking the option "**Keep me signed in".**

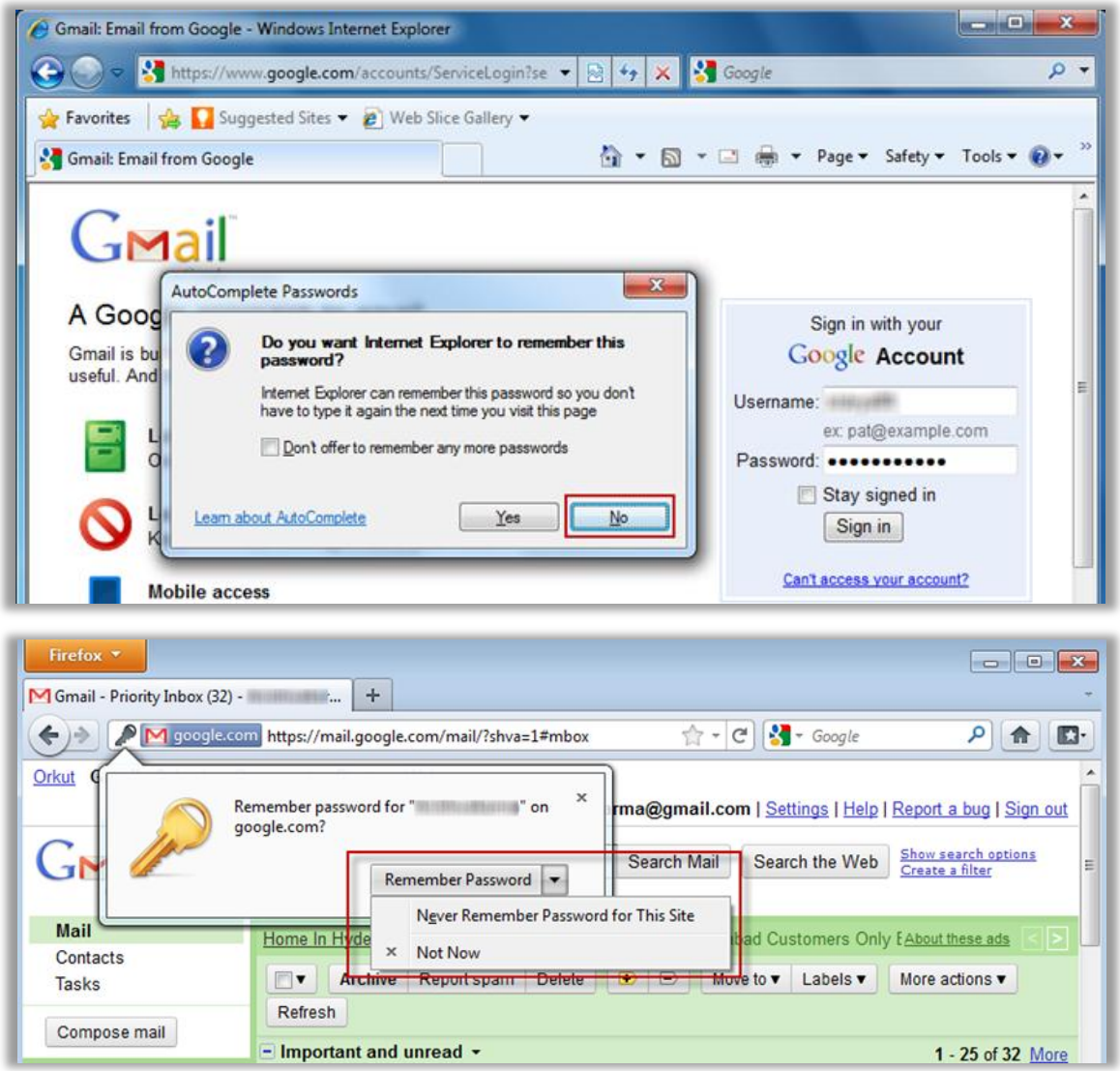

Figure 06-09: Selecting Do Not Allow the Browser to Remember Any Password

Securing File Downloads

Users can configure the download settings in Internet Explorer to set permissions to download files from the Internet. This setting controls whether Internet Explorer should allow downloads or not. File downloads can either be enabled or disabled.

- To configure the download settings for Internet Explorer, click **Tools → Internet Options → Security.**
- Select the **Custom Level** button in the **Security Settings** window.
- In the **Downloads** settings, enable the **File download,** and **Font download** options.

- Click **OK** to save the settings.

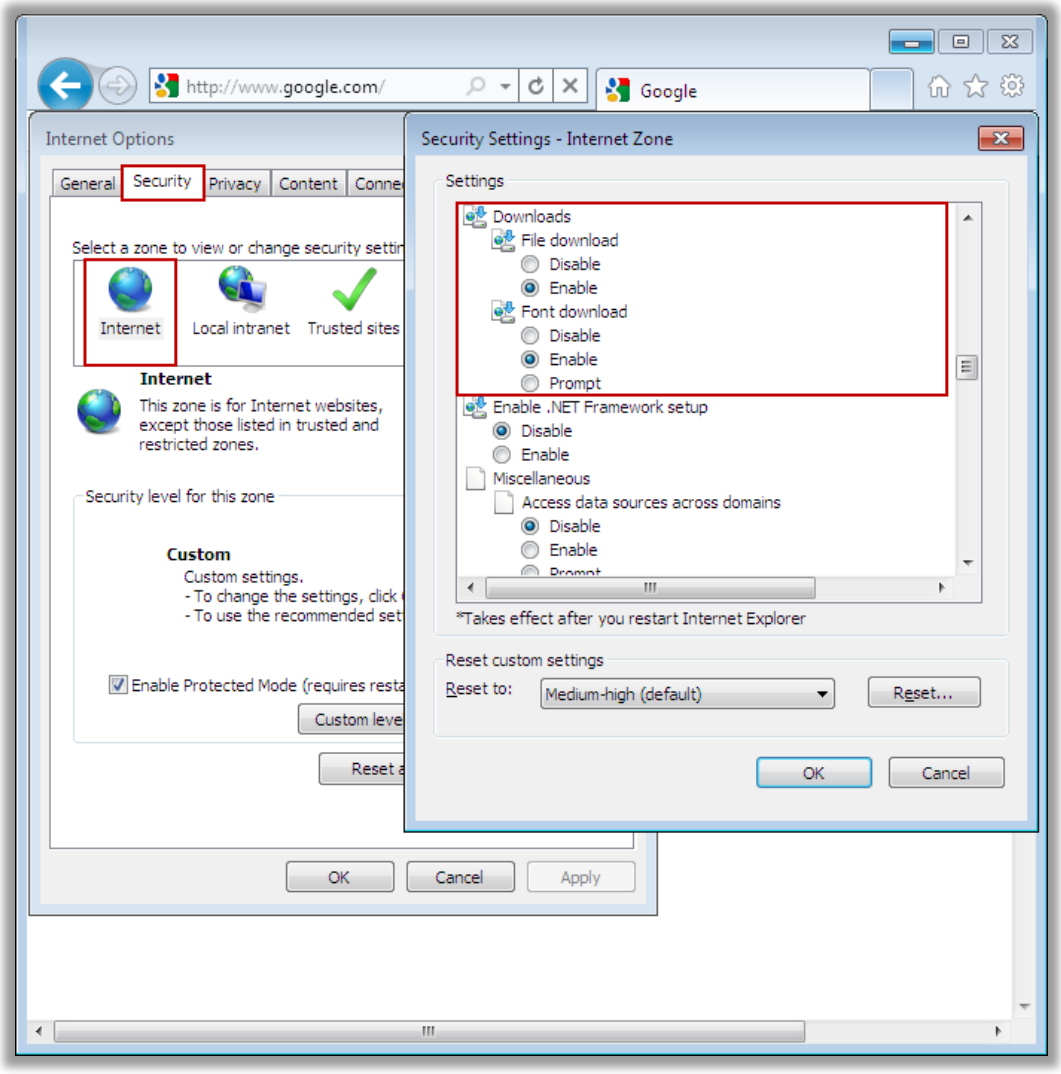

Figure 06-10: Securing File Downloads in Internet Explorer

Mozilla Firefox: Security Settings

Firefox is developed by the award winning global community, Mozilla. It is a secure, fast, and customizable browser.

Securing Firefox settings will prevent attackers from:

- Launch the Mozilla Firefox browser.
- Click **Tools** from the menu and select **Options.**

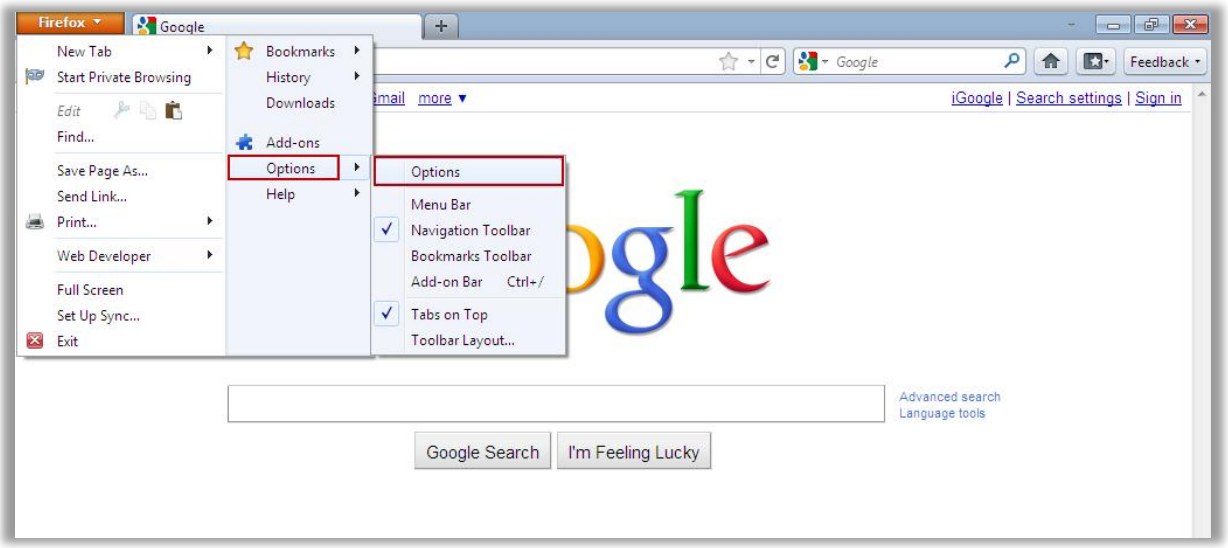

Figure 06-11: Mozilla Firefox Tools Option

Mozilla Firefox: Security Settings

A user can control the level of security by customizing the settings for passwords, cookies, blocking pop ups, loading images, and installing add-ons for a fully empowered web experience. The steps to customize security settings include:

- Select **Security** from the **Options** window.
- Check the option **Warn me when sites try to install add-ons** so that the browser prompts before installing add-ons to the browser.
- Click the **Exceptions** button and enter the URL into the **Address of Website** field and click **Allow** to specify the websites allowed to install add-ons.
- Check the **Block reported attack sites** option to prevent the user from visiting malicious websites.
- Check the **Block reported web forgeries** option for Firefox to actively check whether the sites visited may be an attempt to mislead the user to provide personal information.
- Uncheck the **Remember passwords for sites** option to prevent the browser from remembering passwords for the login pages visited.

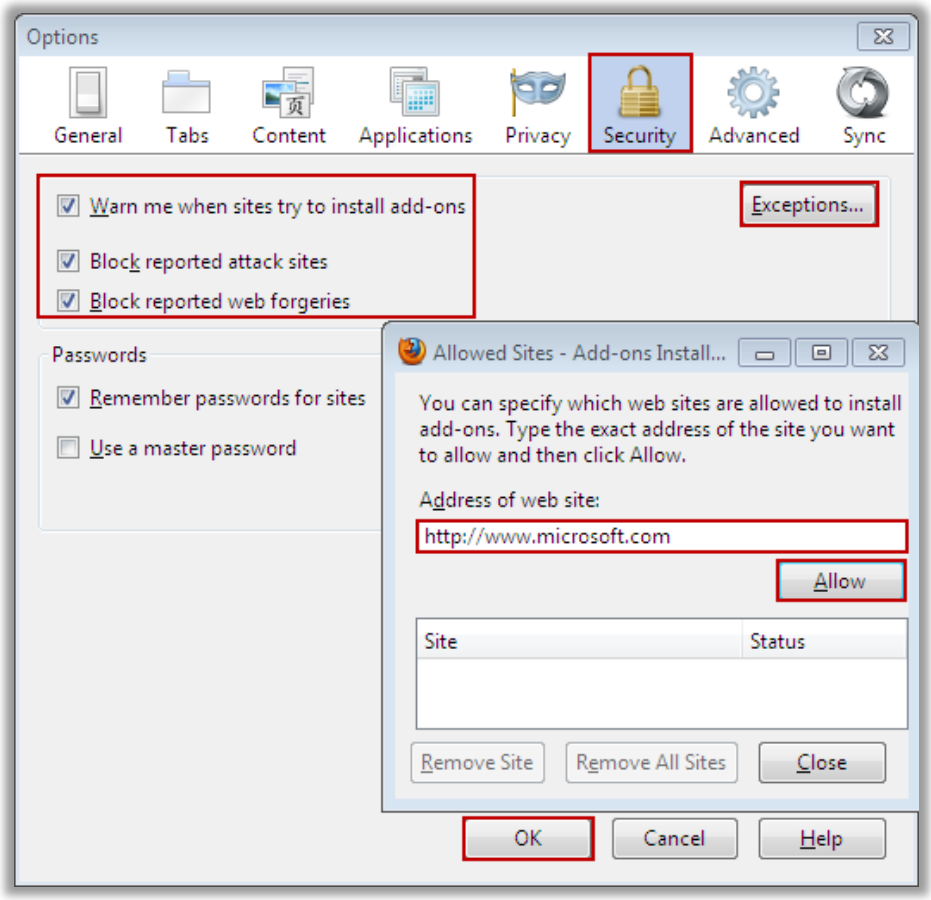

Figure 06-12: Mozilla Firefox Security Settings

Mozilla Firefox: Privacy Settings

Firefox is the open source browser designed and maintained by Mozilla Corporation. It offers speed, security, and customizable features. To set the privacy settings in the browser, follow these steps:

- Select **Privacy** in the **Options** window.
- Firefox allows the users to choose if they want the browser to remember their history. The user may select the option **Never remember history** to maintain privacy.
- Click **Clear your recent history.**
- Select the time range to clear the history.
- Check the options required to clear the history and click **Clear Now.**

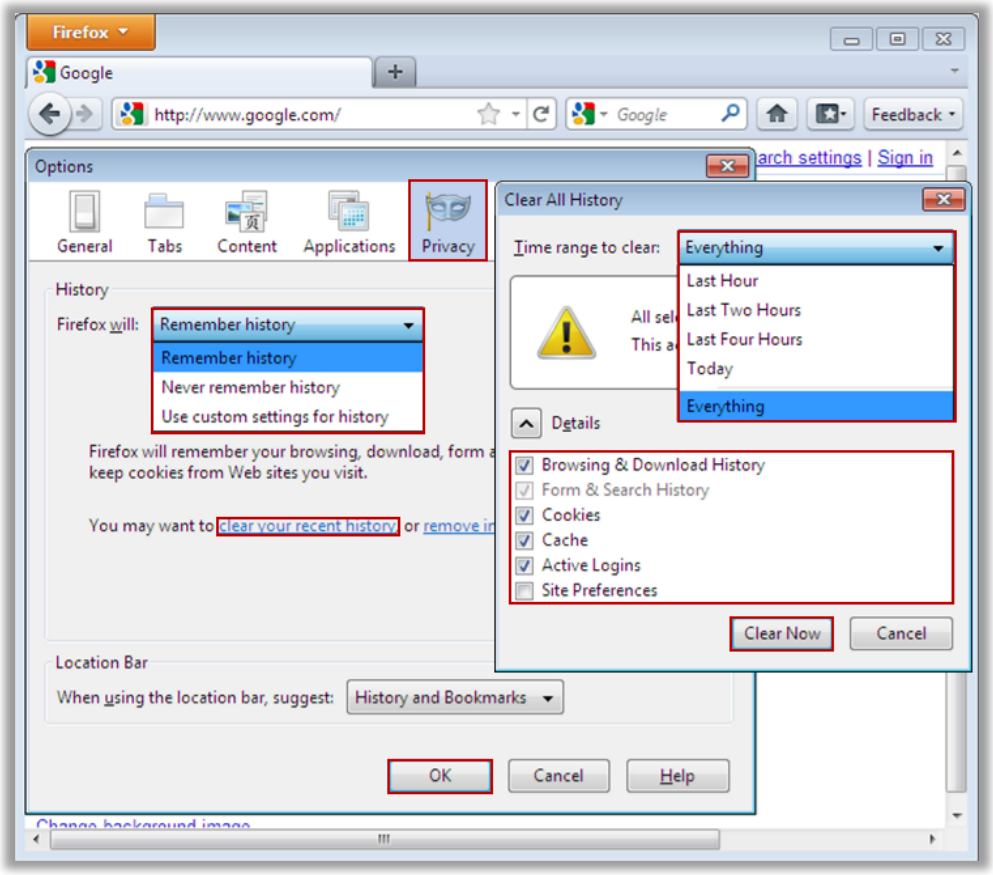

Figure 06-13: Mozilla Firefox Privacy Settings

Securing File Downloads

Most Internet users are facing problems with insecure downloads. To easily secure downloads:

- Do not accept file downloads from unknown members on the Internet.
- The downloads might contain malware that degrades computer performance.
- In Firefox, files are downloaded to **My Documents→ Downloads** by default.
- Configure the browser settings to prompt before downloading files to specify where the file should be saved.

To configure the download settings for Mozilla Firefox:

- Navigate to **Tool→ Options→ General.**
- Always check the option **Always ask me where to save the file** to allow the browser to ask before downloading a file to the desired location.
- The browser downloads the file to the default location without any intimation if this option is unchecked.

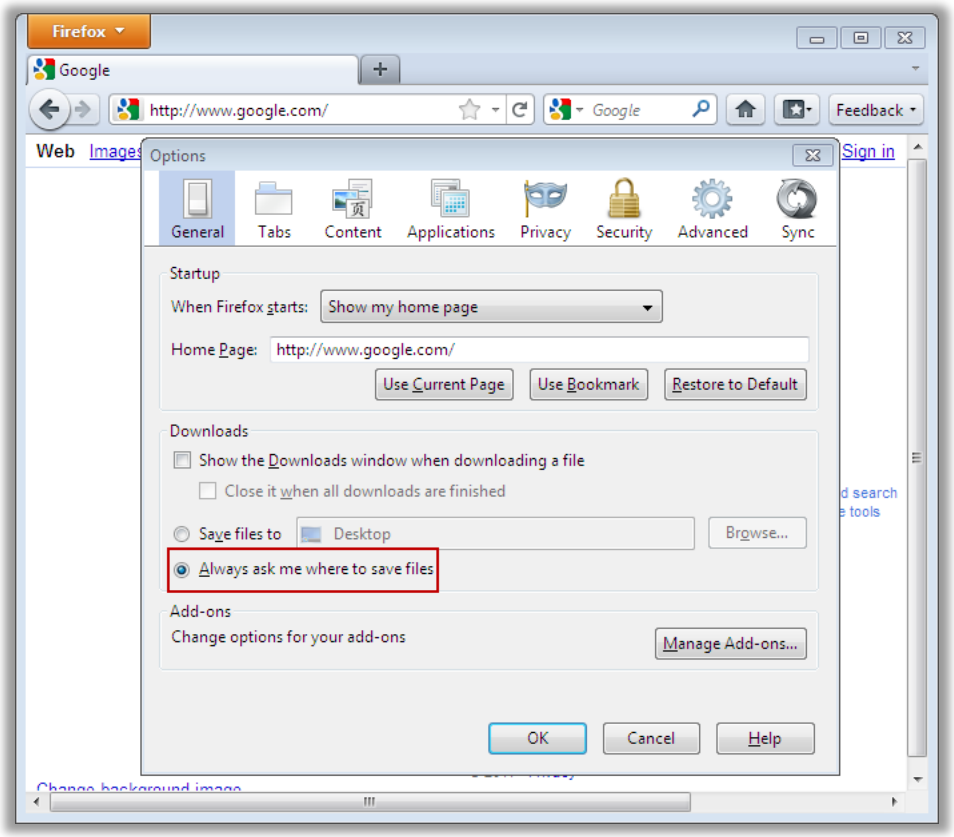

Figure 06-14: Enabling the Option Always ask me before where to save files

Installing Plug-Ins

Installing the missing Plug-ins helps the browser to perform special functions that let a user view special **graphic formats**, and **play multimedia** files and **animated content** in Firefox. For example, plug-ins is needed for applications such as Adobe Reader, Adobe Flash Player, QuickTime, Java, RealPlayer, Shockwave, etc.

To download the plug-in, the user should check that the home source is secure.

- An **Install Missing Plug-ins** message appears when the user opens a website.
- Displaying files or animation on the web page requires installing an application.
- Check whether the missing plug-in is secure.
- Scan the plug-in using anti-virus software before installing it on the system.

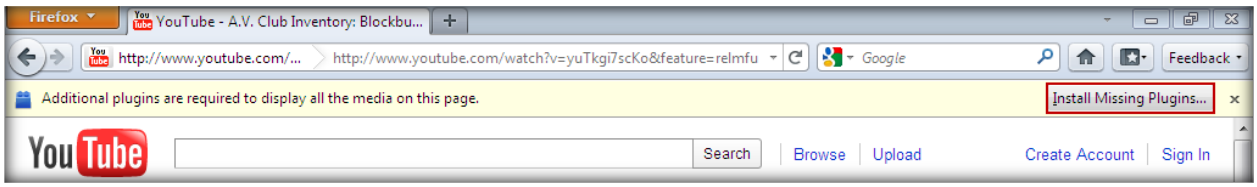

Figure 06-15: Installing Missing Plug-in Window

Google Chrome Privacy and Security Settings

Google Chrome is developed by Google. It utilizes a web kit layout and application framework. Google Chrome comes with security methods to protect a user while browsing the web. Many of the Google Chrome features, such as the web pages you are visiting, use a user's personal information. However, to improve and safeguard his or her web experience, a user should understand what information is being used by the browser and how.

To adjust the privacy settings, follow these steps:

- Launch Google Chrome.
- Click marked icon, then select **Options.**

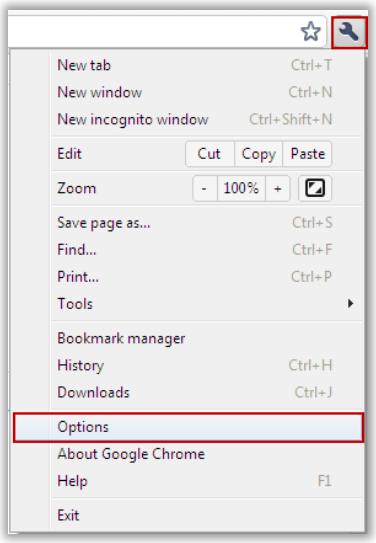

Figure 06-16: Google Chrome Privacy and Security Settings

Google Chrome: Privacy Settings

Google Chrome is provided with advanced privacy settings. With these settings, a user can adjust his or her browser to a high level of security.

- Click the **Under the Hood** tab in the **Google Chrome Options** window.
- Under **Privacy**, check the desired web services.
- Check the **Use DNS pre-fetching to improve page load performance** option.
  - DNS pre-fetching stands for domain name system pre-fetching.
  - When the user visits a webpage, Google Chrome can look up or pre-fetch the IP addresses of all links on the webpage.
- Check the option **Enable phishing and malware protection** to prevent the browser from opening phishing websites and attack sites that contain malware.

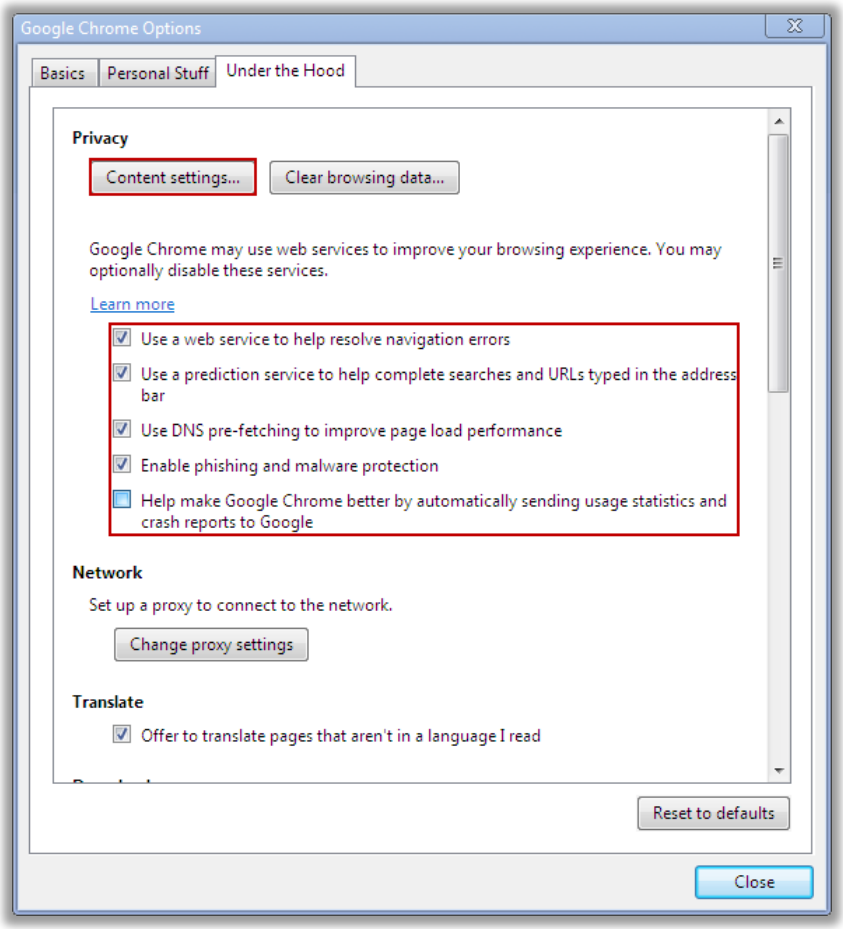

Figure 06-17: Google Chrome Options

Google Chrome: Security Settings

Google Chrome includes features to help protect a user's system from visiting malicious websites. Google Chrome uses advanced technologies like **Safe Browsing**, **sandboxing**, and **auto-updates** to help protect the user against threats like phishing and malware attacks. Whenever a user visits a malicious website, Google Chrome warns the user by prompting a warning message before the user actually visits the website that is suspected to be malicious or fraudulent. To adjust the security settings, follow these steps:

- Secure Sockets Layer (SSL) is an Internet protocol used by many websites to ensure safe data encryption and transmission.
- The SSL setting in web browsers is turned on by default.
- Some websites require an older version of SSL 2.0. Check the **Use SSL 2.0** option in such conditions.
- Check the **Check for server certificate revocation** option to turn on real-time verification for the validity of a website's certificate for extra security.

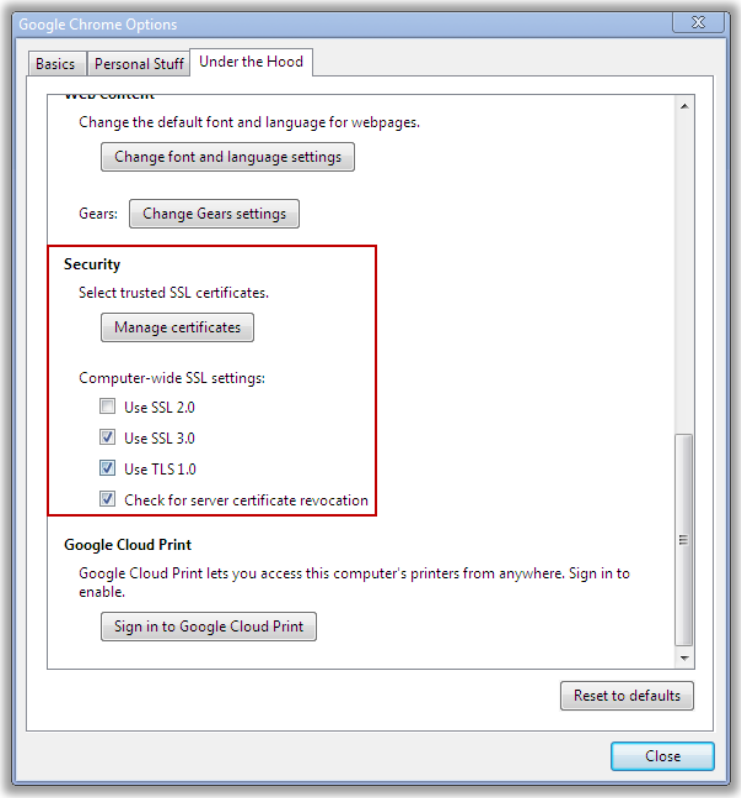

Figure 06-18: Google Chrome Security Settings

Apple Safari: Security Settings

By default, Safari is set to display a few web features, such as some movies, animation, and web applications. A user may wish to turn off these features to help protect privacy from possible security risks on the Internet. The Safari browser contains features equivalent to those in Firefox, with some differences. Change the security settings by following these steps:

- Launch the Safari browser.
- To change the settings, select the marked icon and select **Preferences.**

Figure 06-19: Apple Safari Security Settings

Apple Safari: Security Settings

Security settings instruct the browser to follow certain instructions and decide what actions to allow when accessing websites. These settings prevent malicious sites from running malicious scripts and making changes to a PC without your consent. To configure security settings in Safari browser:

- Select the **Security** tab in the **Preferences** window
- The **Web Content** section permits the user to enable or disable various forms of scripting and active content.
- It is recommended to accept cookies only from sites visited.
- Checking **Ask before sending a non-secure form to a secure website** option allows the browser to warn the user before opening any website that is not secure.

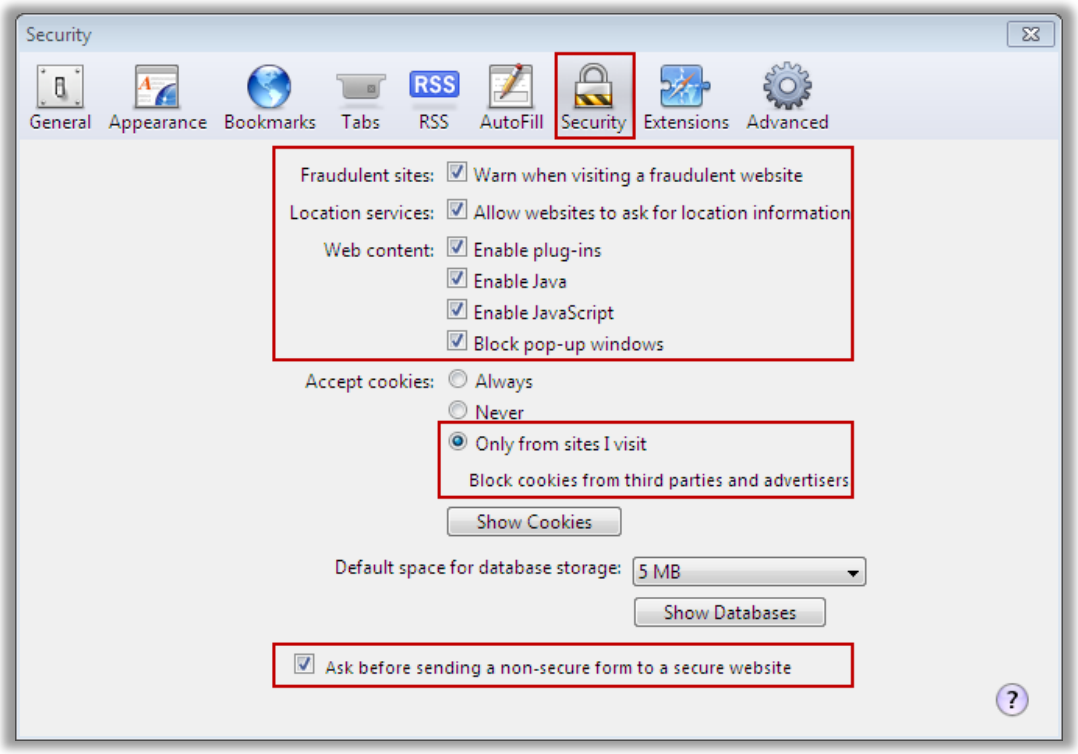

Figure 06-20: Apple Safari Security Settings

Testing the Browser for Privacy

It is necessary to test the browser to evaluate the status of the network and the system.

- Test the browser to check the privacy of the Internet connection and the information that websites can learn about the user.

- This information can be used to display web content based on things such as country of origin and web browser.
- The test:
  - Checks for pop-ups.
  - Traces the user's IP address.
  - Checks for browser plug-ins those are re-installed.
  - Determines the owner of the domain associated with the user's IP address.
  - Checks whether a firewall is blocking the computer.

To test the browser privacy:

- Step 1: Go to http://privacy.net/analyze/ in any browser.
- Step 2: Click **Click here to take the browser test and analyze the privacy of the user's Internet connection.**
- Step 3: See the results displayed in the browser.

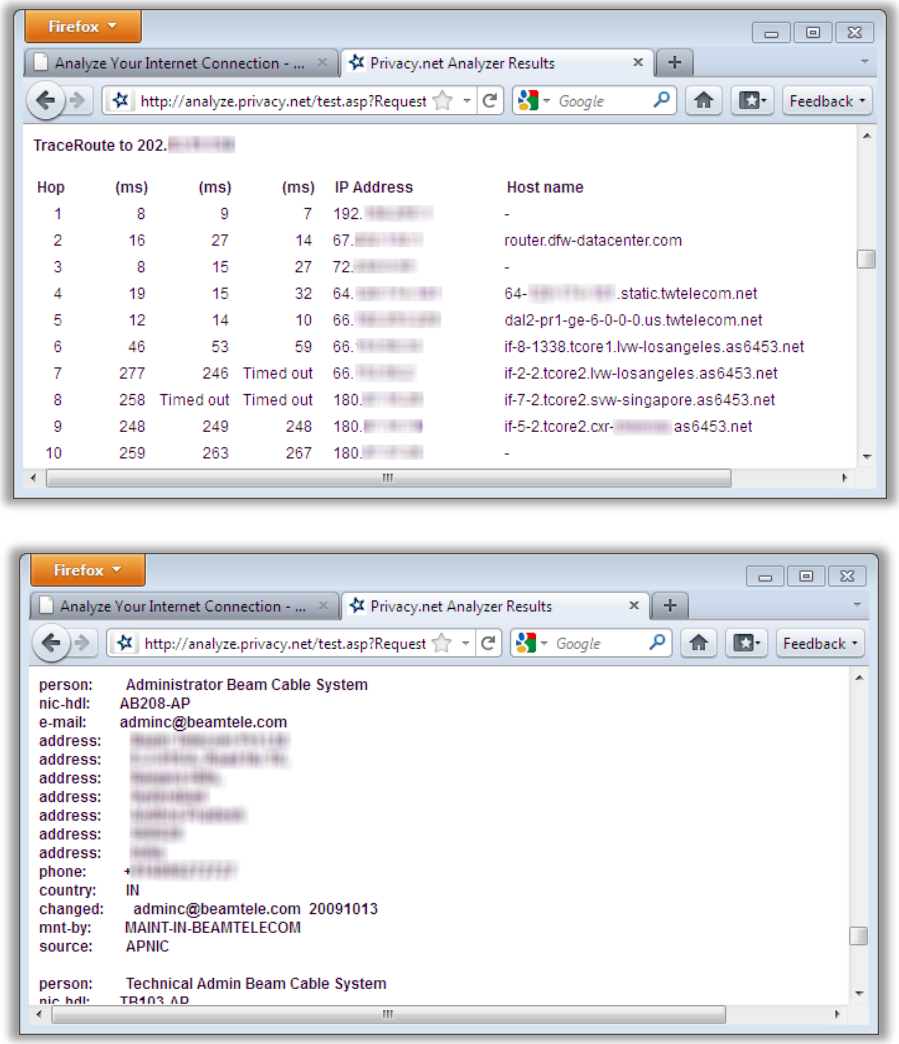

Figure 06-21: Testing the Browser for Privacy Screenshots

IM

Instant messaging (IM) allows the user to interact with other people on the Internet like any other **communication systems** such as telephone, emails, and more, using a software application. Through instant messaging, the user can keep a categorized list of friends. Instant messaging features include:

- **Chat:** A user can create chat rooms to organize the online friends.
- **Web Link Sharing:** A user can share web links with the online friends in less than a few seconds.
- **Video Sharing:** A user can share the video with online friends.
- **Image Sharing:** A user can see the images stored in his or her friend's system.
- **Voice Chat:** A user can talk with the online friends.

Instant Messaging Security Issues

Using Instant Messaging (IM), users can not only transfer text messages but they can also transfer various files. Attackers can use IMs to **transfer viruses**, worms, and other malware to victim machines. IMs can also pave the way for providing an access point for a **backdoor Trojan** and help an attacker **bypass** the desktop and **firewall** restrictions. Instant messaging provides faster and better means of interactive communication than emailing. Yet, it has some security issues, such as:

- **IM worm**
  - An IM worm harms a computer and locates all contacts in the IM address book.
  - The worm is self-replicating and spreads to all contacts present in the IM users' contact list.
- **Social engineering**
  - Social engineering depends on human interaction that involves **tricking people** through instant messaging and getting their personal information.
- **SPIM**
  - Spam over IM (SPIM) is spam delivered through instant messaging instead of email.
  - SPIM is an easier option to spread malware such as viruses, worms, and Trojans to a system.
  - SPIM can affect business systems just like spam.

Instant Messaging Security Measures

These security measures will protect the user from threats such as identity theft and other attacks related to personal information.

- Do not provide personal information on IMs.
- Do not accept links received from unknown persons over IM.
- Block users who send unsolicited web links.
- Use a strong password.
- Do not check the **Remember Password** option.
- Sign out of the application after using it; if not, others may use your login.

Searching the Web

Use search engines to search for desired content. A user can use periodicals, bookstores, and online web links to research a certain topic or content.

- Search engines display numerous web pages.
- All web pages resulting from search engine are not secure.
- To filter the malicious search results, use an antivirus application as an add-on to the browser and enable it.
- To use add-ons in Mozilla Firefox browser, navigate to **Tools→ Add-ons → Get Add-ons.**

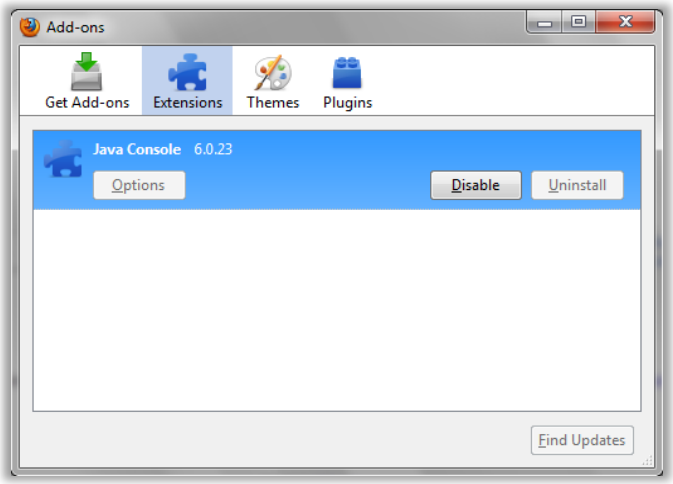

Figure 06-22: Firefox Add-ons Window

- The anti-virus application scans web pages for the presence of malware and indicates those pages that are safe to open from the numerous search pages displayed in an Internet search.
- Avoid opening webpages that are considered dangerous by the anti-virus application.

Online Gaming and MMORPG

Online Gaming

A personal computer (PC) game is played on a personal computer rather than on a gaming console or arcade machine. The games are designed by game developers in collaboration with game artists.

PC gaming started commercially as early as the 1960s with the first computer game "**Spacewar!**" released in the United States, which led to the foundation of an entertainment industry and the growth of the PC gaming market.

The advent of high-speed Internet had given rise to online gaming where players from different corners of the world are **connected**. Online gaming became popular as interest in broadband connections grew. Although dial-up connections can be used for online gaming, broadband connections are more suitable for gaming, as dial-up connections create a "lag" between players. Online games require a game server that connects gamers, and allows **real-time interaction**. Game servers allow the players to customize their settings. North America alone houses 510,000 game servers.

MMORPG

Online games connect **multiple players** and facilitate single-player online gaming. Online games are classified as:

- **First-person shooter** games, in which multiple players play against each other.
- **Real-time strategy** games, in which gamers are automatically matched against each other and allowed to form communities.
- **Browser games** in which people use sophisticated browsers with technologies such as Flash or Java.

Massively Multiplayer Online Role-Playing Game (MMORPG) is a type of computer **role-playing** game in which many players interact with one another within a **virtual** game world. MMORPGs are popular worldwide, and the revenues for these games add up to over a billion dollars. In MMORPGs, also known as online games, players can meet other players, become friends, engage in battle, fight evil, and play. Some of the most popular MMORPG games include World of Warcraft, EverQuest, Asheron Call, Ultima Online, and City of Heroes. MMORPGs are available to gamers for an annual or monthly **subscription fee** in the range of $10–15.

South Korea reportedly has the most MMORPG subscriptions as well as an increasing number of game addicts. This has become a **major concern for parents** around the globe. Apart from becoming addicts, these gamers are prone to risks such as **identity theft**, **cyberbullying**, and more.

Online Gaming Risks

With the online gaming industry churning out billions of dollars in revenue, it has become a target for attackers. Apart from money, online games also offer abundant personal information that attackers may use against the gamers. The risks from online games include:

- Interactions with potential fraudsters who may **trick gamers** into revealing their personal/financial information
- Computer intruders **exploiting security vulnerabilities** in the games or the gamer's PC to take over the machine and launch attacks on other computers
- Online and real-world predators, who **trick infant gamers** into cyber crimes
- **Viruses**, **Trojans**, computer **worms**, and spyware that attackers install on a gamer's computer to collect confidential information

Insecure or Compromised Game Servers and Game Coding

Attackers may exploit vulnerabilities in the game server to break into or crash the server. By **exploiting the vulnerabilities**, attackers can control a user's machine remotely and use it to attack other machines or install malware, such as Trojan horses, adware, or spyware, or steal personal information from the computer.

If the software at the game server is compromised, then the computers connected to the server can also be compromised. In reality, any game that requires a network connection poses more risk to security than a game that does not require a network connection.

The vulnerabilities in the game server and in the game code can be used by attackers to:

- Steal game passwords
- Steal information from the gamer's computer
- Cheat gamers
- Impersonate other gamers
- Money fraud
- Damage files in the gamer's computer
- Cause denial-of-service, where genuine gamers cannot play the game
- Remotely control the gamer's computer
- Launch attacks on other computers
- Install programs such as a Trojan horse, adware, or spyware

Game codes often are not tested as thoroughly compared with tests done on commercial software. This is why games often are plagued by bugs. These bugs are the vulnerabilities that

the attacker may use to **crash the game**, **steal information** from the gamer, or use a computer to launch attacks on other computers.

Social Risks

Computer games were one's solitary activities. But with the advent of MMORPGs, multiple players from across the globe are connected. This resulted in the formation of groups, forums, and chats.

An attacker may use the vulnerabilities in the game server or take control of a gamer's machine, and use the **social interaction** that is rampant on online games to steal personal information.

The social risks that come with online gaming include:

- Social engineering
- Identity theft
- Protection schemes
- Cyber prostitution
- Virtual mugging

Apart from these risks, there are also major concerns over the addiction of gamers to online games. Of particular concern is gamers' decreased social interaction in the real world. Gamers tend to be consumed by the virtual world to the point where they do not bother with a social life. This results in health concerns and affects academics.

Social Engineering

Social engineering is an attack in which human interaction is used to gather confidential information from the victim.

Attackers may try to **trick a gamer** into installing software on his or her computer that can be used to control the computer, monitor gamers' online activities, or launch attacks on other computers. They may **direct** the gamer **to a compromised website** that offers bogus game patches or downloads.

They may offer a bonus or help in the game in exchange for players' passwords or other game information. Gamers looking for ways to make play easier respond to such offers and give away their personal information.

Attackers may also send **phishing emails**, supposedly from the game server administrators, which invite the player to authenticate his or her account via a website linked in the message.

Protection Schemes, Cyber Prostitution, and Virtual Mugging

Protection Schemes

Protection schemes are similar to cyber bullying. A protection racket or scheme is an **extortion scheme** in which a criminal organization forces individuals to pay extortion money for services rendered. This money serves as a protection against external threats from rival organizations or anyone else.

South Korea has reportedly seen the emergence of protection schemes in online gaming. In these schemes, members of criminal organizations allegedly join a game as gamers. They then warn weaker players in the game to pay or face **negative consequences** in the game.

The negative consequences may include:

- Killing gamers' characters
- Stolen passwords
- Real or virtual money being paid as ransom or game characters being surrendered to the criminals to avail protection

Cyber Prostitution

Online games are being used for cyber prostitution where customers/gamers pay money for cybersex.

The game "Second Life" is driven by user-created content. This content includes entertainment at nightclubs, including cybersex. Users allegedly earn $30 for a few hours.

In "The Sims online", a massively multiplayer online (MMO) game, a 17-year-old developed a "cyber brothel," in which gamers pay Sim-money (Simoleans) for cybersex. The gamer's account was eventually cancelled.

According to a user of the games, some teenagers engaged in "cyber-prostitution" (i.e., simulated sex by the characters of the game). But, the game architecture limited the ability of the participants in performing such acts. Therefore, the users found another alternative; they traded cybersex chat in **exchange for real** or **virtual money**.

Virtual Mugging

Virtual crime or in-game crime refers to a criminal act in MMORPG games. Virtual mugging was coined when some players of "Lineage II" used bots (web applications that run automated tasks over the Internet) to defeat other gamers and take their items. These items were later put on sale in online auctions.

Virtual mugging occurs when a gamer **uses bots** to force someone else's game characters to submit to the virtual criminal's character. The game characters are then exchanged later for real or virtual money as well as other virtual objects.

The bots can perform tasks in a game, such as beating up a character repetitively or quickly. The bots thus give virtual muggers an **unfair advantage**. Experts believe that virtual mugging does not seem to be slowing down as the money involved is too great for criminals to stay away from online games. Reports also suggest that some online scammers use "**sweatshops**" in which people monitor teams of bots in order to generate money while avoiding bot traps.

How the Malicious Users Make Money?

Financial gain is the **ultimate motive** of cyber-criminals who steal from the gamers. They always look for ways to exchange stolen items while staying unnoticed. Stolen items such as passwords, virtual items, or virtual characters are put on sale on websites such as EBay or forums. These are sold to other gamers for real or virtual money. The cyber-criminal may ask the gamer for ransom in return for this information.

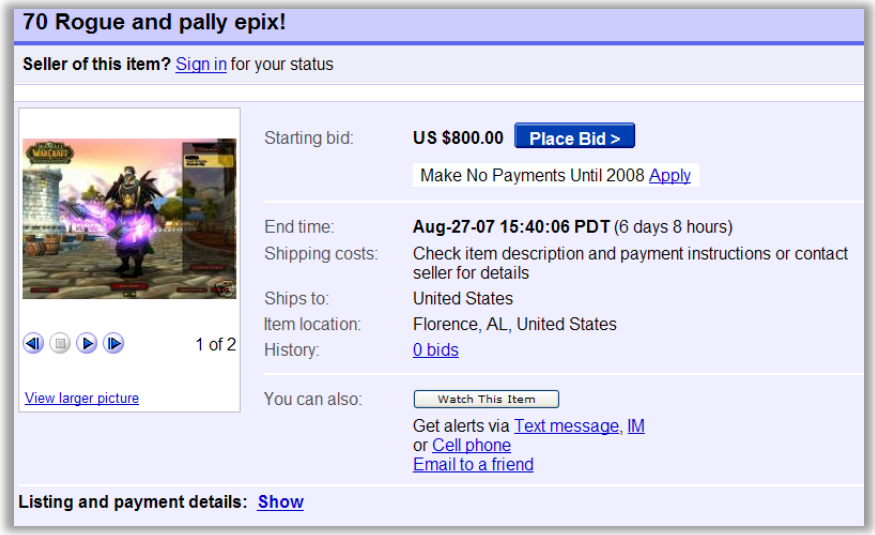

Figure 06-23: Game Characters for Sale on EBay

Security Practices Specific to Gaming

Recognize "Administrator Mode" Risks

Some games require that the gamer be in administrator mode. Playing a game in administrator mode allows an attacker to **gain control** of the computer.

With faster broadband connections, vendors can now sell games online. It is up to the user to ensure that the game is downloaded from reputed vendors because the downloaded files may **contain malware** that runs when the gamers execute the downloaded files.

The malware may then allow an attacker to steal personal information or take control of the computer to launch attacks on other computers.

Recognize Risks due to ActiveX and JavaScript

Browser games require the gamer to install certain plug-ins to play the game. The user has to ensure that the plug-ins are downloaded from **reputable sites**. Running plug-ins in administrator mode may install malicious programs on the computer.

Instead of using the administrator account, the gamer is advised to browse the Internet or play the games with a "**User Account**," which may deny an attacker access to administrator rights.

Some of the games played over the web require that ActiveX or JavaScript are enabled. The gamer should be aware that enabling these features leads to vulnerabilities. These features should only be enabled for games downloaded from trusted websites.

Play Only at the Game Site

Attackers may send links to **phishing sites** over chats in forums of online games. These sites may look strikingly similar to the original. An unsuspecting user may give his/her game account details (user name and password) to login to the **fake website**. The account details are thus stolen from the user.

The user has to be aware of such phishing sites and should not click any links provided in the game forums.

A gamer can play games at the game site to avoid any phishing websites. The user may also save Internet browsing for later. If the game needs to be played in administrator mode, the user can play at the gaming site and then switch to the user account for browsing the Internet. This reduces the risk of visiting a malicious website when playing a game.

Pay Attention to Firewall Management

A firewall is hardware, software, or a combination of both that is used to prevent unauthorized programs or Internet users from accessing a private network and/or a single computer.

A home computer faces the same cyber threats as an organization does. Therefore, a firewall **must be installed** to protect the network from potential threats from attackers.

The firewall acts as a filter for the information that comes into a network through the Internet. If the information is flagged as potentially harmful, the firewall blocks it.

Playing certain multiplayer games may require changing the **firewall settings** to allow information from the game to get through to the users' computers. Every time the permission settings are changed on the firewall, the risk of a computer security breach increases.

Firewalls may be designated by the gamer, with fellow gamers' IP addresses set as "trusted" to avoid any interactions with an attacker.

Child Online Safety: Risk Involved Online

Internet browsing is useful and informative, but at the same time, children are **exposed to risks** online. A few risks involved when a child gets online include:

- Misdirected searches
- Stealth sites and Misleading URLs
- Online sexual harassment
  - Child pornography
  - Grooming
  - Cyber bullying
- Stealing personal information
  - Social networking websites
  - Unsolicited emails
  - Chat rooms

Misdirected Searches

Children should be protected from online threats and **know how to secure** their systems. Even if parents take every precaution to protect the child online, they may be negated when the child is unconsciously led to visit harmful sites. **Search engines** use terms known as "**Meta variables**" to index a website. When a user searches for websites, the search engine displays the results using the Meta variables. For example, a sports website may be indexed by

the Meta terms “soccer,” “football,” “scores,” and so on. Pornography websites add popular search terms to their Meta variable list to redirect web traffic to their site. A porn site may use the words “sports,” “school,” “movies,” and so on to lure children to their websites. Unless **filtering software** is used, the search engines cannot distinguish between the search requests of an adult and a child.

Stealth Sites and Misleading URLs

Stealth sites are Internet businesses websites that use misleading URLs to increase their traffic. Pornographic websites thrive on increased web traffic. These sites use common typo errors to lure visitors to their sites. Children may come across similar domain names when they search for particular information. **Online predators** purchase domain names such as the “.com” equivalent of a “.gov” or “.org” website, knowing that web suffers would end up at their website if they mistype.

Child Pornography, Grooming, and Cyberbullying

Child Pornography is a **serious crime**. A growing number of children access the Internet all over the world. Rapidly expanding computer technology and the Internet has given access to the **production** and **distribution** of child pornography.

Child pornography is defined by the United States Federal law as *“*a visual depiction of any kind, including a drawing, cartoon, sculpture, or painting, photograph, film, video, or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where it depicts a minor engaging in sexually explicit conduct and is **obscene**, or depicts an image that is, or appears to be, of a minor engaging in graphic bestiality, sadistic or masochistic abuse, or sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex.”

As children spend more of their time on the Internet, they are increasingly becoming prey to child abusers/pornographers. Child pornography begins with the production of pornographic materials such as porn images and videos. Offenders enter into correspondence with children through online instant messaging or chat rooms. They emotionally attract the prospective victim and befriend them. After establishing a steady relationship, they introduce children to pornography by providing images and videos that have sexually explicit material. Pornographers make use of poor children, disabled minors, and sometimes neighborhood children for sexual exploitation.

The distribution of porn material is also a serious crime. The Internet has made the distribution of illegal material simple. Pornographers resort to newsgroups, Internet Relay Chat, web-based groups, email, webcams, and peer-to-peer technology to distribute pornographic material. Downloading such images is also considered a crime.

Grooming

Grooming is one of the major risks that a child faces online. "Grooming" is an act of **befriending** and establishing an emotional connection with children. Child grooming is used for lessening a child's inhibitions and preparing them for child abuse. Child grooming is also used to draw children into sexual **exploitation** and child prostitution. Most of the people have become online sexual predators by browsing the Internet. They are so involved in preying on children online that they can easily trap a child into having a sexual conversation.

Offenders target a child's attention, kindness, and affection. They converse about studies, jobs, and sports and try to offer advice to befriend the child. They also offer gifts, money, and try to impress the child. After a few conversations, they introduce sexual content in their conversation and show them sexually explicit material.

Cyber Bullying

Cyber bullying is a major risk that both children and adults are facing nowadays. Cyber bullying is the same as grooming. Cyber bullying occurs when a child, preteen, or teen is **threatened**, harassed, and/or embarrassed through the Internet, mobile phones, or social media. It involves a death threat or a credible threat of serious bodily harm for the child.

Individuals resort to cyber bullying to vent their frustration, hatred, or anger, or simply do it for the pleasure. To prevent cyber bullying, parents should **educate** their **children** about cyber bullying and teach them to respect other children. Parents together with schools/teachers should educate children on **cyber-ethics** to stop them from resorting to cyber bullying.

To keep the problem from getting worse, parents should tell their children to ignore any messages from bullies, or to change their email address and user name on social networking sites. Signs that indicate that the child is a victim of cyber bullying include:

- The child feels upset after using the computer.
- The child may refuse to step out of the house or to go to school.
- The child may draw away from friends and family.
- The child may become uncomfortable when he/she receives an email, text message, or IM.

Role of the Internet in Child Pornography

A child's easy access to the Internet is **one of the primary reasons** that contribute to child pornography. Although the Internet does have positive aspects such as learning and networking, the negative aspects seem to outweigh the positives.

Negative aspects of the Internet for children include:

- Access to pornographic material

- Complete anonymity and privacy
- Various web services such as email, news groups, and chat rooms that facilitate the sharing of pornographic materials
- Cost-effective transfer of pornographic materials and access to pornographic materials anytime and anywhere
- Transfer of pornographic materials in various formats that can be stored on different digital storage devices

Effects of Pornography on Children

There are many ways that pornography may harm children. Since pornography has got a new path to enter into the homes and schools through the Internet, it is important for the parents and teachers to look at the ways how pornography can **potentially harm** children.

- The victims of child pornography are subjected to various physical and mental illnesses, **anti-social behavior**, and more.
- Child victims also suffer from **depression**, anger, withdrawal, and other psychological problems.
- They experience mental weakness such as:
  - Guilt and feeling responsible for the abuse and betrayal
  - Sense of powerlessness and worthlessness
  - Low self-esteem

Risks Involved in Social Networking Websites

Social networking websites are used to interact with friends, but they can also lead to **cyber bullying**. If the information on social networking sites is not maintained properly, the user may be at risk of **losing personal information**. Some risks involved in social networking websites include:

- People can view profiles, scraps, photos, and videos of other people on that website. If personal photos and videos are not displayed on the profile, then they remain secure.
- A child should only reveal the proper amount of information in their profile. The problem occurs when the child provides too much information.
- Online predators may get information such as an email, telephone number, and residential address, as well as hobbies, interests and much more, from their profile. Online predators may use this information for cyber bullying, **identity theft**, or cyber exploitation.

Unsolicited Emails

Unsolicited bulk email is the practice of sending unwanted emails to consumers or Internet users. These emails often contain inappropriate content such as links to pornographic material or advertisements to adult products.

The attackers may also use these emails to steal personal information. The emails may compel children to visit a website or download a software program, and then **steal personal information**.

Apart from this, online predators may also steal information related to bank accounts and credit cards by providing various payment options.

Chat Rooms

A chat room is a place where people communicate depending on their interests. Nearly, all instant messengers offer chat rooms according to the interests of the user such as sports, movies, arts, and so on.

Online predators may use **social engineering** techniques in chat rooms to elicit personal information from children. Social engineering techniques enable an online predator to divert a child's attention toward them and ask him or her to have a private conversation on an instant messenger. They may use chat rooms to build contacts with children and then lead them into various types of cybercrimes. They may also use chat rooms to send links to websites with **inappropriate content**, such as pornography. Online predators may also send malicious links to children, which can result in the computer being infected with malware.

Determining if Children Are at Risk Online

Online activities are always fraught with risks, especially for children. Often, children may not be aware of such risks and thus may not express their problems or issues related to **online risks**. This may lead them to suffer in silence. Parents can determine if their children are at risk by looking for the following symptoms:

- The child spends more time on the computer.
- Pornographic material is present on the child's computer.
- The child receives phone calls and/or gifts from unknown persons.
- The child turns off the monitor or quickly changes the screen when a parent enters the room.
- The child looks depressed and does not show any interest in talking with family or friends.

Protecting Children from Online Threats

Children are prone to online threats. They should learn about the dangers of extended online time. However, parents should:

- Ensure that the child is **aware** of online threats.
- **Monitor** what the child does on the computer.
- Use caller ID phones to determine who is calling the child and block the numbers that are suspicious.
- Monitor the child's access to all types of live electronic communications such as chat rooms, instant messages, Internet Relay Chat, and so on.
- **Restrict access** to the malicious and porn websites using Internet content-filtering software.
- **Inspect** the child's social networking profile; look closely at what information they have posted on his or her member profiles and blogs, including photos and videos.
- Check credit card statements each month for any unusual charges that may indicate unauthorized purchases by the stranger or child.
- Notify the police if someone who met the child online starts calling them, sends gifts, or tries to lure them.
- In addition, parents should also ensure that the child does not:
  - Provide personal information such as their name, address, phone, or name of their school
  - Meet anyone from their online acquaintances without permission
  - Open emails from unknown senders
  - Share their photo/videos with strangers over the Internet

Encourage Children to Report

To protect their child from online predators, threats, and so on, parents should encourage their children to:

- **Report** any inappropriate behavior they encounter online
- Come to them if they are being bullied or are facing online predators
- Speak to a trusted individual such as an aunt, uncle, or older sibling if they are uncomfortable talking to their parents
- Ensure that the child knows how to report any inappropriate behavior they encounter online

How to Report a Crime?

Source: http://www.justice.gov

Internet-related crime, like any other crime, should be reported to appropriate law enforcement authorities at the local, state, federal, or international levels, depending on the scope of the crime. Citizens who are aware of federal crimes should report them to local offices of federal law enforcement.

Internet crimes can be reported at http://www.ic3.gov/complaint/default.aspx by clicking **Report Internet Crime**

Security Software Checklist

Children can be protected from online threats by installing appropriate security software on the child's computer. The features of the security software should include:

- **Web blocking** to help prevent the child from viewing inappropriate content
- **Program blocking** to help block games, peer-peer file sharing, and so on
- **Email blocking** to help block unknown email addresses and prevent children from communicating with people they met online through email
- **Time limits** to help control the amount of time the child spends on the computer
- **IM features** to help in recording and monitoring the child's IM chats, thus helping parents determine if their child is engaged in an inappropriate dialogue with unknown persons
- **Usage reports** to provide a timely report on the child's Internet usage and IM history to monitor the child's online interactions
- **Video filtering** to ensure that the child does not view inappropriate videos on sites such as YouTube but at the same time allows the child to view useful/fun videos
- **Social networking features** to help in recording and monitoring the content the child posts online and to determine if the child is being bullied

KidZui

Source: http://www.kidzui.com

KidZui is a free web browser, search engine, and online playground for kids. It has a number of games, websites, videos, and photos reviewed by parents and teachers. It eliminates the need for parents when kids are online

KidZui features:

- Search is essential for kids, as they learn about the things that will make them productive adults. KidZui search is tailored to children's requirements. KidZui search

provides suggestions and spelling correction, search results, and graphical presentations.

- KidZui has a number of games, websites, videos, and photos reviewed by parents and teachers. Children can browse this content easily and independently.
- Children can share and tag content in KidZui.
- The KidZui community is tailored for children as they learn about the things that make them productive adults. It is safe with no chat, no written text, and no email. The KidZui community allows kids to:
  - Add and block friends
  - Share content with friends
  - Ping friends to say "Hi"
  - See friends come online and their interests

KidZui features for parent:

- The KidZui Parent account eliminates the need for parents to constantly watch over their child's shoulder when they are online. Parents can view everything from searches to blocked websites and favorites to time spent online. Parents can share content, set limits, and stay connected to their child's online life.
- Parent reports show a child's online activities, interests, favorites, searches, friends, and time spent on KidZui. Parent reports are located in the parent account and are sent to the parent once a week by email.
- Parent tools personalize and set limits to the child's KidZui account. Parent tools are located in the parent account.

Actions to Take When the Child Becomes an Online Victim

The moment a child becomes an online victim, the parents should encourage the child to:

- **Ignore any contact** from the online predator or cyber bully
- **Avoid logging** into the website where the bullying occurred
- **Block** the **offender**'s email address and screen name so that they cannot contact the child again
- Change the child's online information
  - Delete the social networking accounts if necessary
- **Report** the offense to the Internet Service Provider (ISP)
  - Also report to the offender's ISP

Internet laws

Cyber space is a vast terrain and the Internet has benefitted its users tremendously. The concept of affiliate marketing and networking has allowed Internet users to earn money through these websites. The Internet allows users to start their own business by using business sites, educational and news websites, and entertainment websites.

Because cyber space is so vast, it has also become a breeding ground for hackers, cyber-criminals, and other trouble makers. Therefore, **supervision** of the Internet has become necessary, which Internet laws provide. Although no amount of supervision may stop hackers or cyber-criminals, who work from hideouts in any corner of the world, Internet laws do bring in a sense of responsibility, safety, and discipline among the netizens.

Need to know Internet laws:

Internet laws are comparatively new and most Internet users know little about them. This makes the Internet a ground that should be treaded carefully. A user may simply download a song or a movie from a website and be sued for **copyright infringement**. He or she may post a picture or video of a friend and then find themselves in a lawsuit for **infringing privacy**. A user may even be sued for **defamation** for posting something against an individual over a blog/forum.

Therefore, it is important that users know the Internet laws:

- To leverage disputes against e-commerce vendors, fraudsters, and Internet criminals
- To understand what they can and cannot post on the Internet
- To be able to legally use the immense content present over the Internet

Scope of the Internet laws:

Internet laws safeguard users against many immoral acts. The nature of communications over the Internet poses a threat to the privacy of Internet users. Communications between electronic mail users are routed through a series of computer networks and therefore are vulnerable to interception by anyone in that network. The Internet laws cover a wide number of issues akin to the offline world. Issues that the Internet laws cover include:

- Defamation
- Intellectual property
- Patents
- Copyrights
- Privacy infringement
- Child protection
- Trademarks
- Credit card fraud
- Data theft and so on

Laws Internet users should know:

Internet laws vary from country to country. But because the Internet is a world with thin boundaries, a criminal from any country can be charged for an Internet crime by any other country. Major Internet laws that a user should know to stay safe and responsible on the Internet include:

- USA PATRIOT Act
- Children's Online Privacy Protection Act (COPPA)
- The Digital Millennium Copyright Act
- CAN-SPAM Act
- Computer Misuse Act 1990
- European Union Data Protection Directive (95/46/EC)
- Data Protection Act 1998

USA PATRIOT Act

Source: http://www.justice.gov

USA PATRIOT Act is the acronym for United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act. The act was passed as a response to the September 11, 2001, terrorist attacks on the United States.

TITLE II-**Enhanced Surveillance** Procedures, section 216 of the Patriot Act, gives law enforcement authorities access to dialing, routing, and signaling information. The mention to routing information exclusively refers to Internet use for either email or Internet browsing. The Internet routing information would include websites that the suspect may have visited and what he/she has done while browsing the website. According to the act, law enforcement authorities have access to the email packets (includes email content).

Under the act, the government can compel the ISP to release **subscriber information** that includes:

- Customer name
- Customer address
- Mode of payment
- Credit card information
- Bank account information

Section 212 of the Act allows the ISPs to voluntarily **disclose customer information** including the customer records and all electronic transmissions (email and voice transmissions). The ISPs may choose to reveal customer information if they believe that there is risk of death or bodily injury to an individual or group. Section 220 of the act allows for **nationwide search warrants**

for email. This gives the authorities the right to search a suspect without having to go to the place of the ISP.

The act:

- Authorizes pen register and trap and trace orders for electronic communications (e.g., email)
- Authorizes nationwide execution of court orders for pen registers, trap and trace devices, and right of entry to stored email or communication records
- Considers stored voice mail such as stored email
- Allows authorities to **interrupt communications** to and from an intruder within a computer system
- Supports collaboration between law enforcement and foreign intelligence investigators
- Establishes legality for certain communication privacy breaches by government personnel
- Concludes the authority present in many of these provisions and many foreign intelligence amendments with a sunset provision

Children's Online Privacy Protection Act (COPPA)

Source: http://www.coppa.org

The Children's Online Privacy Protection Act (COPPA) April 21, 2000, is relevant to the online collection of personal information from **children below the age of 13**.

The act dictates:

- What a website owner must include in the **privacy policy**
- When and how the **verifiable consent** can be requested from the parents
- The responsibility of the website owner in protecting the **children's online safety** and privacy

Who must comply with COPPA?

Every website operator who runs an **online service** targeted at children **below the age of 13** years or runs a general website and has knowledge that **private information** is being collected **from children** should comply with COPPA. The Federal Trade Commission (FTC) determines if a website is targeted at children below age 13 by checking the content of the website, age of the models on the website, language, children-oriented features on the website, and more.

To determine whether an individual or group of individuals is the "operator" of the website, the FTC considers who owns and controls the information and pays for the maintenance of the website, the contractual information, and so on.

Personal information:

COPPA applies to the **child data** collected online that helps to identify a child. The data/information may include:

- Full name
- Contact information—address, email, and telephone numbers
- Hobbies and interests
- Information collected through cookies or other tracking methods

Privacy policy:

The operator must include a link to the **privacy policy** of the website on the home page. The link should be prominent and clear, and the operator may use the following specifications:

- Large font size
- Varying colors on a contrasting background so that the link stands out
- A link presented in a small font and does not contrast with the background is not considered distinguishable and prominent

The privacy policy should include the following information:

- The name and contact information of all the operators collecting/maintaining the personal information
- The kind of personal information that will be collected
- How the operator intends to use the personal information
- Whether the operator releases the personal information to third parties
- If the parents' consent is required for releasing information to third parties
- The procedure parents should follow to control their children's personal information

According to the act, the operator should:

- Notify the parents that he or she intends to collect their children's information
- Ask for parents' consent before releasing information to third parties/public disclosure
- Inform parents about the internal use of personal information
- Inform parents if there are any changes in the privacy policy

Parental consent is not required when the website owner collects the email address of the parent/guardian or the child to:

- Provide notice and seek consent
- Ask a one-time request from a child and then delete it
- Respond more than once to a specific request—for example, for a subscription to a newsletter

- Protect the safety of the child participating on the site
- Protect the security or liability of the site or to respond to law enforcement, if necessary, and is not used for any other purpose

The Digital Millennium Copyright Act

Source: http://www.copyright.gov

The Digital Millennium Copyright Act (DMCA) 1998 was signed into law by President Clinton. According to the act, any **infringement** of the copyrighted material is a criminal offense.

The DMCA is divided into five titles:

- Title I, the "WIPO Copyright and Performances and Phonograms Treaties Implementation Act of 1998," implements the WIPO treaties.
- Title II, the "Online Copyright Infringement Liability Limitation Act," limits the liability of online service providers for copyright infringement when engaging in certain types of activities.
- Title III, the "Computer Maintenance Competition Assurance Act," excuses making a copy of a computer program for the purposes of maintenance or repair from the law.
- Title IV contains six provisions, relating to the functions of the Copyright Office, distance education, the exceptions in the Copyright Act for libraries and for making ephemeral recordings, "webcasting" of sound recordings on the Internet, and the applicability of collective bargaining agreement obligations in the case of transfers of rights in motion pictures.
- Title V, the "Vessel Hull Design Protection Act," protects the design of vessel hulls.

Highlights of DMCA

The act originally received support from software and entertainment industries but was opposed by scientists and academicians.

Highlights of DMCA include:

- **Circumventing** any anti-piracy measures built into commercial software is a crime.
- The production, sale, or distribution of code-cracking tools to illegally copy software is banned.
- **Cracking** copyright-protected software to perform encryption research and test computer security systems is permitted.
- Nonprofit libraries, educational institutions, and so on are excused from the act under certain circumstances.
- ISPs are excused for simply transmitting information over the Internet.

- ISPs are, however, required to remove copyright infringing materials from user websites.
- Webcasters are required to pay a **licensing fee** to recording companies.

CAN-SPAM Act

Source: http://www.ftc.gov/, http://www.fcc.gov

In 2003, the U.S. Congress passed the Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act to control spam. According to the act, the Federal Communications Commission (FCC) adopted rules that forbid sending unnecessary commercial email messages to wireless devices without prior permission.

The CAN-SPAM Act defines commercial messages as those for which the primary purpose is to advertise or promote a commercial product or service. The FCC's ban does not cover "transactional or relationship" messages or notices to facilitate a transaction that the consumers have already agreed to.

The messages include statements about an existing account or warranty information about a product that a customer has purchased. The act establishes the standards for sending commercial email.

The CAN-SPAM Act:

- Defines the rules for commercial email
- Establishes the requirements for commercial messages
- Gives recipients the right to stop emailing them

Each email that violates CAN-SPAM Act is subject to penalties of up to $16,000.

CAN-SPAM's Main Requirements

CAN-SPAMs main requirements include:

- The use of false or misleading email header information is prohibited.
- The use of email subject lines that are misleading/deceptive is prohibited.
- If the message is an advertisement, the senders are required to clearly disclose that information.
- The senders should tell the recipients how they can opt out of receiving more emails.
- Senders should honor the recipient's opt-out request within 10 business days.
- If a third party is sending emails on the organization's behalf, they should monitor what is being sent to the recipient.

Computer Misuse Act 1990

Source: http://www.opsi.gov.uk

The Computer Misuse Act 1990 was enacted by the UK Parliament.

The act makes certain activities illegal such as:

- Hacking into other user's computers
- Misusing software
- Helping an attacker gain access to secured files/documents in another user's computer

The act defines three computer misuse offenses:

- **Unauthorized access to computer material**:
  - An individual is found guilty if:
    - He/she attempts to gain control of or take a program from another user's computer
    - The computer or program he/she targets is unauthorized
    - The individual is aware of the offense
    - The intent of an individual to commit an offense under this section need may not be directed toward:
    - A particular program or data
    - A program or data of any particular type
    - A program or data held in any particular computer
    - The individual, if found guilty under this section, could be imprisoned up to 6 months, have to pay a fine, or both.
- **Unauthorized access with an intent to commit** or facilitate the commission of further **offenses**:
  - A person is guilty of an offense under this section if he or she commits an offense under section 1 with an intent to commit an offense to which this section applies or facilitates the commission of such an offense
  - This section applies to offenses for which the sentence is fixed by law, or for which the individual is 21 years of age or older
  - An individual may be guilty of an offense under this section even though the facts are such that the commission of the further offense is impossible
  - An individual guilty of an offense under this section will be accountable for:
    - A prison term 6 months or over, on conviction
    - A prison term of 5 years, a fine, or both on indictment
- Unauthorized modification of computer material:
  - An individual is guilty of an offense if:

- He or she modifies the contents of a computer, when unauthorized
- He or she has the knowledge and intent when the offense is carried out

- The individual modifies the content of the computer:
  - To hinder the functioning of any computer
  - To deny access of any program or data on any computer
  - To make the data or programs on any computer unreliable
- The intent does not have to be directed at:
  - A particular computer
  - A particular program/data/ program
  - A particular modification
- The act holds if the offense is temporary or permanent
- Modification of the contents of the computer will not be considered damaging a computer if the computer or other media are not physically damaged
- A person guilty of an offense under this section shall be accountable for:
  - A prison term of 6 months, fine, or both on conviction
  - A prison term of 5 years, fine, or both on indictment

European Union Data Protection Directive (95/46/EC)

The protection of individuals with regard to the processing of personal data and on the free movement of such data

Source: http://eur-lex.europa.eu/

The European Parliament and the Council of the European Union's directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data provides guidelines to European Union member states for **individuals' privacy and data protection**. The directive regulates the processing of personal data regardless of whether such processing is automated or not. The key highlights of the directive include:

SECTION I: PRINCIPLES RELATING TO DATA QUALITY

Member States shall provide that personal data must be:

(a) processed fairly and lawfully;

(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes;

(c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the

purposes for which they were collected or for which they are further processed, are erased or rectified.

SECTION II: CRITERIA FOR MAKING DATA PROCESSING LEGITIMATE

Member States shall provide that personal data may be processed only if:

(a) the data subject has unambiguously given his consent; or

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or

(c) processing is necessary for compliance with a legal obligation to which the controller is subject; or

(d) processing is necessary in order to protect the vital interests of the data subject; or

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed.

SECTION V: THE DATA SUBJECT'S RIGHT OF ACCESS TO DATA

Member States shall guarantee every data subject the right to obtain from the controller:

(a) without constraint at reasonable intervals and without excessive delay or expense:

(b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;

(c) notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort.

Data Protection Act 1998 (UK)

Source: http://www.legislation.gov.uk

The Data Protection Act 1998 is a United Kingdom Act of Parliament which defines UK law on the processing of data on identifiable living people. It is the main piece of legislation that governs the **protection of personal data** in the UK. Although the Act itself does not mention privacy, it was enacted to bring UK law into line with the European Directive of 1995 which required Member States to **protect people's fundamental rights** and **freedoms** and in particular their right to privacy with respect to the processing of personal data. The main highlights of the law include:

- Data may only be used for the specific purposes for which it was collected.
- Data must not be disclosed to other parties without the consent of the individual whom it is about, unless there is legislation or other overriding legitimate reason to share the

information (for example, the prevention or detection of crime). It is an offence for Other Parties to obtain this personal data without authorization.

- Individuals have a **right of access** to the information held about them, subject to certain exceptions (for example, information held for the prevention or detection of crime).
- Personal information may be kept for no longer than is necessary and must be kept up to date.
- Personal information may not be sent outside the European Economic Area unless the individual whom it is about has consented or adequate protection is in place, for example by the use of a prescribed form of contract to govern the transmission of the data.
- Subject to some exceptions for organisations that only do very simple processing, and for domestic use, all entities that process personal information must register with the Information Commissioner's Office.
- The departments of a company that are holding personal information are required to have adequate security measures in place. Those include technical measures (such as firewalls) and organisational measures (such as staff training).
- Subjects have the right to have factually incorrect information corrected (note: this does not extend to matters of opinion)

Module Summary

Internet security involves protecting user data and information from unauthorized access when connected to the Internet.

Scan file downloads with updated antivirus software to check for the presence of malware.

To filter the malicious search results, use an antivirus application as an add-on to the browser and enable it.

Online gaming has become a popular pastime, especially because of high-speed Internet and emerging technology.

If the software at the game server is compromised, the computers connected to the server can also be compromised.

Parents may take all precautions to protect the child online, but they could be negated when the child is unconsciously led to visit harmful sites.

The Internet laws protect its users from immoral/indecent acts and from privacy breaches on the Internet.

Internet Security Checklist

The following is a list of the best practices a user should follow for safer Internet communications:

- ☐ Regularly update your operating system and other installed applications
- ☐ Set up a firewall to control the flow of information
- ☐ Ensure that you have the latest web browser installed on the system and update it regularly
- ☐ Install a safe browsing tool that warns about reported phishing sites and blocks access to the addresses
- ☐ Ensure that you are connected to a secured network when using a wireless network
- ☐ Never respond to unsolicited email offers or requests for information

Internet Security Checklist

The following is a list of the best practices a user should follow for safer Internet communications:

- ☐ Do not click the links sent by unknown users
- ☐ Do not download files from unknown sources
- ☐ Do not give out personally identifiable information when registering with websites/applications
- ☐ Do not click any pop-ups that appear while browsing websites
- ☐ Regularly scan your system for viruses, worms, Trojans, spyware, key loggers and other malware using antivirus
- ☐ Update the antivirus application on a regular basis

Internet Security Checklist

The following is a list of the best practices a user should follow for safer Internet communications:

- ☐ Use strong passwords and change them at regular intervals
- ☐ Disconnect from the Internet if anything suspicious is found on the computer

- ☐ Always check the Address bar for correct URL
- ☐ Always check the website certificate, SSL padlocks and HTTPs
- ☐ Do not enable ActiveX and JavaScript features
- ☐ Regularly back up the important files
- ☐ Remove unnecessary protocols from the Internet interface
- ☐ Check router or firewall logs to identify abnormal network connections to the Internet

Guidelines for Parents to Protect Children from Online Threats

To protect a child from online threats, parents should:

- ☐ Talk to their children about what they do on the computer
- ☐ Get a profile on the social networking site the child is on
- ☐ Be informed of the challenges of social networking
- ☐ Review the list of the child's friends
- ☐ Check if anyone is trying to impersonate the child online