E-mail

Objectives : At the end of this lesson you shall be able to
- **state the hotmail services offered**
- **explain MSN outlook express and its tools**
- **explain popular search engines**
- **state the FAQs about hotmail.**

Hotmail: MSN Hotmail is the world's largest provider of free Web-based e-mail. Hotmail is based on the premise that e-mail access should be easy and possible from any computer connected to the World Wide Web.

By adhering to the universal HyperText Transfer Protocol (HTTP) standard, Hotmail eliminates the disparities that exist between different e-mail programs. Sending and receiving e-mail from Hotmail is as easy as going to the Hotmail web site at http://www.hotmail.com, or by clicking on the Hotmail link at http://www.msn.com, signing in, and sending an e-mail message.

Hotmail is the web-based e-mail provider, which means you can send and receive messages from any computer connected to the Internet. You can use Hotmail from home, work, school, an Internet cafe, a friend's house or any other computer in the world with an Internet connection. Your messages are stored in a central location, so your Inbox will always be up to date. This is great for people who use more than one computer, travel frequently, or don't even own a computer.

Advantages of Hotmail

Get a permanent e-mail address: When you create a Hotmail account, you choose a permanent e-mail address that will never change as long as you continue to use Hotmail. This is great for people who: Want to switch Internet Service Providers. Your Hotmail address will be the same no matter how you access the Internet, so you don't have to worry about retrieving messages from your old address or notifying friends, family and associates of a new e-mail address. You are free to select any Internet Service Provider that suits your needs.

When you leave town for travel, you may no longer have access to your ISP's e-mail account. But with Hotmail, your friends will always know where to reach you.

Your e-mail is private and secure: When you sign up for Hotmail, you choose your personal ID and password. The only way you can access your account is by using the password you selected. This means that only you will have access to your Hotmail account, even if you use a computer at a public terminal or a friend's house. Because the messages in your Hotmail account are stored securely at a central location, you don't have to worry about losing important information if something happens to your computer. Hotmail is strongly committed to keeping your personal information confidential.

Hotmail is fast and easy to use: Hotmail is recognized world wide as the best Web-based e-mail service. It is also stated that 'while others provide similar services, none can match Hotmail's general ease of use'. If everything is fine, it takes less than a minute to get started on Hotmail and its pages are so worked out to load quickly knowing that the users time is valuable.

Get an additional e-mail account for FREE:Hotmail offers everyone the opportunity to get a free e-mail account. Hotmail can offer e-mail accounts for free because it places banner advertising on some of its pages. Some Internet Service Providers charge a monthly fee for additional e-mail accounts. Hotmail lets an unlimited number of people use a single Internet Service Provider account and have a free, personal e-mail account.

Keep your personal e-mail separate from your work e-mail: People who use e-mail for work will find it convenient to keep their personal messages separate from their work messages. You can use Hotmail for your personal correspondence and your company's e-mail system only for business messages. Additionally, you don't have to store personal e-mail on your company's servers. All messages in your Hotmail account are securely stored in a central location that you access via the Internet with the password you select.

Outlook Express

Microsoft Outlook Express puts the world of online communication on your desktop. Whether you want to exchange e-mail with colleagues and friends or join newsgroups to trade ideas and information. Some of the tools offered by outlook express are;

Manage multiple mail and news accounts: If you have several mail or news accounts, you can use them all from one window. You can also create multiple users, or identities, for the same computer. Each identity gets its own mail folders and Address Book. The ability to create multiple accounts and identities makes it easy for you to keep work separate from personal mail and also between individual users.

Browse through messages quickly & easily: Using the message list and preview pane, you can view a list of messages and read individual messages at the same time. The Folders list contains mail folders, news servers, and newsgroups, and you can easily switch between them. You can also create new folders to organize and sort messages, and then set up message rules so that

incoming mail that meets your criteria automatically goes to a specific folder. You can also create your own views to customize the way you look at your mail.

Keep your mail on a server so you can view it from more than one computer: If your ISP uses an IMAP mail server for incoming mail, you can read, store, and organize your messages in folders on the server without downloading the messages to your computer. That way, you can view messages from any computer that can connect to that server.

Use the Address Book to store and retrieve e-mail addresses: You can save names and addresses in your Address Book automatically by simply replying to a message or by importing them from other programs, by typing them in, by adding them from e-mail messages you receive, or by searching popular Internet directory services (white pages). The Address Book supports Lightweight Directory Access Protocol (LDAP) for accessing Internet directory services.

Add a personal signature or stationery to your messages: You can insert essential information into outgoing messages as part of your personal signature, and you can create multiple signatures to use for different purposes. For more detailed information, you can include a business card. To make your messages look more attractive, you can add stationery patterns and backgrounds, and you can change the color and style of the text.

Send and receive secure messages: You can digitally sign and encrypt messages by using digital IDs. Digitally signing your message assures recipients that the message is really from you. Encryption ensures that only intended recipients can read a message.

Find newsgroups that interest you: Looking for a newsgroup that matches your interests? You can search for newsgroups that contain keywords or browse through all of the newsgroups available from your Usenet provider. When you find a newsgroup you want to view regularly, add it to your Subscribed list so you can find it again easily.

View newsgroup conversations efficiently: You can view a newsgroup message and all of the responses without reading an entire message list. When you view the list of messages, you can expand and collapse conversations to make it easier to find what interests you. You can also use views to display only the messages you want to read.

Download newsgroup messages for offline reading: To use your online time efficiently, you can download messages or entire newsgroups, so you don't have to be connected to your ISP to read messages. You can also download message headers only for offline viewing and then mark the headers of the messages you want to read; then the next time you are connected, Outlook Express downloads the message text. You can also compose messages offline and send them the next time you reconnect.

Some important (Top 8) recommendations for staying safe and secure when you're online are listed below;

- Change your password often. The quick act of changing your password can ensure your e-mail remains private. In addition,passwords that use both letters and numbers are harder to break.
- Don't share your password. Most e-mail administrators will not ask for your password. Do not be duped by malicious e-mails asking you for your password. This is a well-known, although not-too-common trick designed to fool you into sharing your password. As a rule, never share it with anyone.
- Never open attachments from unknown sources. They may contain what are known as "letterbombs" or "viruses," which can damage your PC.
- Always remember to sign out when you are done. It's quick, easy and may save your account from unwanted trespassers. If you are using a public terminal, at an internet cafe for example, it is advised that you close the browser you were using when you are ready to end your Internet session.
- Don't reply to unsolicited messages ("spam") mail, or other harassing or offensive mail. By responding, you only confirm that you are a person with an active e-mail address who can be plagued with constant unwanted e-mail solicitations. Instead, forward the unsolicited message to the customer service department of the source's e-mail (usually of a form similar to abuse@[implicateddomain].com). To help control spam, Hotmail provides members with "filters" for incoming mail. These can easily be set up to send certain messages (such as those that include certain words) directly to your online trash can.
- Make sure that you are using the most up-to-date Internet software (e.g. browsers such as Microsoft Internet Explorer or Netscape Navigator). More recent versions often offer enhanced security protection.
- Always use a secure network. Most corporate networks and Internet service providers are protected by administrators who watch for potential security problems and act to protect users from "hackers" (malicious users) who may try to steal personal information that is transferred through the network. Although the risk is small, use caution when on any unfamiliar network.
- Use stations maintained by sources you trust, or ask if the Internet terminal you are using is protected against security break-ins.

A SMALL LIST OF Search Engines

Yahoo.com (http://www.Yahoo.com)

Search.com (http://search.com)

EasySearcher (http://www.easysearcher.com)

AltaVista (http://www.altavista.com)

Excite (http://www.excite.com)

Google (http://www.google.com)

Hotbot (http://www.hotbot.com)

Infoseek (http://www.infoseek.com)

Lycos (http://www.lycos.com)

WebCrawler (http://www.webcrawler.com)

www.all4one.com (This useful tool queries four search engines at once)

www.av.com (Very powerful search engine which gives plenty of results)

www.askjeeves.com (Insted of entering words to search for, just type in your question)

www.rediff.com (Search for anything)

www.bigfoot.com (Looking for someone's email address ? Try here)

www.sawaal.com (All your questions answered)

www.hotbot.com (Useful search engine which helps to find pictures, video or music)

www.indiainfo.com (Info lets you search the web easily)

www.yahoo.com (Search engine which is also the most popular)

mp3.lycos.com (The place to start if you're after music files in the mp3 format)

www.metacrawler.com (Metacrawler puts your search through a host different engines)

www.mirago.co.uk (A search engine eith an excellent selection of shopping links)

www.webferret.com (One of the easiest way to search the web)

www.indiatimes.com (The portal's search engine)

www.webcrawler.com (Let the webcrawler spider to do the searching for you)

www.indonet.net (Excellent Indian search engine with loads of useful search catagories)

www.satyamonline.com (On ISP's site and has good search options)

COMPILED LIST OF INTERESTING FAQ's about HOTMAIL

1 How much e-mail storage space do I get with Hotmail?

Hotmail offers 2MB of storage space. If you do not keep your account below this limit, Hotmail may remove some messages, which cannot be recovered.

If you need additional storage space, there are a few options. You can use the latest version of Microsoft Internet Explorer v5 or above, which includes Outlook Express, which offers you the ability to store e-mails locally. You can send a blank e-mail message to hmoex@hotmail.com for more information on how to use the beta (pre-release) process to store Hotmail messages on your local PC, using Outlook Express.

Also, MSN has introduced Preview 2 of MSN Explorer as an integrated client for MSN services, such as MSN Hotmail. This client allows you to also store Hotmail locally on your machine. This too reduces the amount of storage that you need on hotmail.

2 Can I get Hotmail in different languages?

MSN Hotmail can now be viewed in a variety of languages.

You can make the language of a Hotmail session match the language of the Sign In page used to begin that session. You have your choice of the following languages: English, French, German, Italian, Japanese, Portuguese (Brazilian), and Spanish, and more to come.

3 Can I use Hotmail as a business address?

No. You may not use your Hotmail address as your primary business address. If, however, you work for a company with which you have an e-mail address and you want to use your Hotmail account to send and receive e-mail while away from your computer at work, you are encouraged to do so.

Example of Prohibited Use:

You are an individual who runs a business. You and your employees want to use Hotmail accounts rather than registering and administering your account through a paid ISP.

Example of Allowed Use:

You are a businessperson who travels. You have an account with your company **(yourname@your company.com).** You use your Hotmail account to read and send solicited messages while you are traveling.

Hotmail prohibits account sharing. Since Hotmail is accessible from everywhere in the world, each individual is able to sign up for his or her own personal account. You are encouraged to sign up for an account of your own, to which only you have access. Sharing an account compromises the privacy and security of your e-mail. Each Hotmail user must have his or her individual e-mail account.

4 Is my e-mail really private and secure? (SSL)?

Secure connections (often called SSL, or Secure Sockets Layer) is the industry standard in Web security. It is used primarily for transmitting sensitive information over the Internet. When you have a secure connection between your browser and a Web site, no one else can easily access the data that you send across the connection. Hotmail uses SSL to encrypt your sign-in name, and password, when you log in to give you a high level of security.

It is Hotmail's policy to respect the privacy of its users. Therefore, Hotmail will not monitor, edit, or disclose the contents of a user's private communications unless required to do so by law or in the good faith belief that such action is necessary to:

– conform to the edicts of the law or comply with legal process served on Hotmail;

– protect and defend the rights or property of Hotmail; or

– act under exigent circumstances to protect the personal safety of its users or the public.

5 Can Hotmail protect its users from e-mail viruses?

MSN Hotmail is pleased to offer users McAfee VirusScan for free. Whenever you receive attachments in your Hotmail account, it will automatically scan them with McAfee's popular VirusScan before downloading.

MSN Hotmail recently added the ability to have all attachments you want to send scanned before they can be attached to your outgoing e-mail. So before you upload file to send to another user, it will also be scanned for viruses before you send it, reducing the spread of viruses to Hotmail users and the other recipients of your e-mail.

Remember, to ensure safety, Hotmail recommends that you never open attachments from unknown sources.

6 How do I send images and use e-mail stationery to make e-mail I send more colorful and fun?

(Emoticons/Stationery/RTF)

MSN Hotmail offers users stationery to send fun, colorful messages to family and friends! Always capture the right mood for your messages by selecting one of the many different stationery templates. Use the Stationery Chooser button on the Compose page to view the available stationery choices.

You can also accent your messages by using Rich Text Formatting. The Rich Text Formatting option, also allows you to add emoticons to your e-mail. This new feature allows you to add selected symbols or emoticons to your message. These icons help you convey emotion or add flair within a message.

7 What does it mean when my account is marked "inactive"?

Currently, if you do not sign in to your Hotmail account for 60 days, or if you do not sign-in within the first 10 days, your account will be marked "inactive." Stored e-mail and addresses will be deleted, and inbound mail will be refused. Your Passport will still function, and your Hotmail e-mail name will be reserved. To re-activate your account, simply go to http://www.hotmail.com and enter your Sign-In name and password. You will then be able to once again send and receive e-mail using hotmail. If your account stays "inactive" for over a period of 90 days, it may be permanently deleted.

8 Can I send and receive attachments on Hotmail?

Yes, you can send and receive as many files as you want to a message - up to 1MB (1024K) of attachments.

Attachments sent to your Hotmail account can be downloaded to your personal computer by clicking them. GIF and JPEG images and HTML files are automatically displayed in the browser window.

Chatting, video chatting and using social network sites

Objectives : At the end of this lesson you shall be able to
- **explain chating process**
- **explain video chating process**
- **explain social network services.**

Chatting Process

A web chat is a system that allows users to communicate in real time using easily accessible web interfaces. It is a type of internet online chat distinguished by its simplicity and accessibility to users who do not wish to take the time to install and learn to use specialized chat software. This trait allows users instantaneous access and only a web browser is required to chat. Users will always get the latest version of a chat service because no software installation or updates are required.

Video Chat

In video chat video of both caller and receiver can be seen on screen of both user along with audio. So it gives an impression of face to face interaction though the caller and receiver can be thousands of mile apart.

Social Networking services

A social networking service is a platform to build social networks or social relations among people who, share interests, activities, backgrounds or real-life connections. A social network service consists of a representation of each user (often a profile), his social links, and a variety of additional services. Social networking is web-based services that allow individuals to create a public profile, to create a list of users with whom to share connection, and view and cross the connections within the system. Most social network services are web-based and provide means for users to interact over the Internet, such as e-mail and instant messaging.Social network sites are varied and they incorporate new information and communication tools such as, mobile connectivity, photo/ video/sharing and blogging. Online community services are sometimes considered as a social network service, though in a broader sense, social network service usually means an individual-centered service whereas online community services are group-centered. Social networking sites allow users to share ideas, pictures, posts, activities, events, interests with people in their network.

The main types of social networking services are those that contain category places (such as former school year or classmates), means to connect with friends (usually with self-description pages), and a recommendation system linked to trust. Popular methods now combine many of these, with American-based services such as Facebook, Google+,YouTube, LinkedIn, Instagram, Pinterest, Tumblr and Twitter widely used worldwide; Nexopia in Canada; Badoo, Bebo, Vkontakte (Russia), Delphi (also called Delphi Forums), Draugiem.lv (mostly in Latvia), Hi5 (Europe), Hyves (mostly in The Netherlands), iWiW (mostly in Hungary), Nasza-Klasa, Soup (mostly in Poland), Glocals in Switzerland,Skyrock, The Sphere, StudiVZ (mostly in Germany), Tagged, Tuenti (mostly in Spain), and XING in parts of Europe; Hi5 and Orkut in South America and Central America; Mxit in Africa; and Cyworld, Mixi, Orkut, renren, weibo and Wretch in Asia and the Pacific Islands.

There have been attempts to standardize these services to avoid the need to duplicate entries of friends and interests (see the FOAF standard and the Open Source Initiative). According to experts, the largest social networking users are Asian-Pacific regions with 615,9 million people. A 2013 survey found that 73% U.S adults use social networking sites.

Explaining threats to computers connected to Internet & process of protecting computers from it.

Objectives : At the end of this lesson you shall be able to
• explain threats to computers connected to Internet
• process of Protecting computers from Internet.

A web threat is any threat that uses the World Wide Web to facilitate cybercrime. Web threats use multiple types of malware and fraud, all of which utilize HTTP or HTTPS protocols, but may also employ other protocols and components, such as links in email or IM, or malware attachments or on servers that access the Web. They benefit cybercriminals by stealing information for subsequent sale and help absorb infected PCs into botnets.

Web threats pose a broad range of risks, including financial damages, identity theft, loss of confidential information/data, theft of network resources, damaged brand/personal reputation, and erosion of consumer confidence in e-commerce and online banking.

It is a type of threat related to information technology (IT). The IT risk, i.e. risk affecting has gained and increasing impact on society due to the spread of IT processes.

Web threats can be divided into two primary categories, based on delivery method - push and pull. Push-based threats use spam, phishing, or other fraudulent means to lure a user to a malicious (often spoofed) website which then collects information and/or injects malware. Push attacks use phishing, DNS poisoning (or pharming), and other means to appear to originate from a trusted source.

Precisely-targeted push-based web threats are often referred to as spear phishing to reflect the focus of their data gathering attack. Spear phishing typically targets specific individuals and groups for financial gain. In other push-based web threats, malware authors use social engineering such as enticing subject lines that reference holidays, popular personalities, sports, pornography, world events and other hot topics to persuade recipients to open the email and follow links to malicious websites or open attachments with malware that accesses the Web.

Pull-based web threats are often referred to as "drive-by" threats by experts (and more commonly as "drive-by downloads" by journalists and the general public), since they can affect any website visitor. Cybercriminals infect legitimate websites, which unknowingly transmit malware to visitors or alter search results to take users to malicious websites. Upon loading the page, the user's browser passively runs a malware downloader in a hidden HTML frame (IFRAME) without any user interaction.

Internet security

Internet security is a tree branch of computer security specifically related to the Internet, often involving browser security but also network security on a more general level as it applies to other applications or operating systems on a whole. Its objective is to establish rules and measures to use against attacks over the Internet. The Internet represents an insecure channel for exchanging information leading to a high risk of intrusion or fraud, such as phishing. Different methods have been used to protect the transfer of data, including encryption.

Types of security

Network layer security

TCP/IP which stands for Transmission Control Protocol (TCP) and Internet Protocol (IP) aka Internet protocol suite can be made secure with the help of cryptographic methods and protocols. These protocols include Secure Sockets Layer (SSL), succeeded by Transport Layer Security (TLS) for web traffic, Pretty Good Privacy (PGP) for email, and IPsec for the network layer security.

Internet Protocol Security (IPsec)

This protocol is designed to protect communication in a secure manner using TCP/IP aka Internet protocol suite. It is a set of security extensions developed by the Internet Task force IETF, and it provides security and authentication at the IP layer by transforming data using encryption. Two main types of transformation that form the basis of IPsec: the Authentication Header (AH) and ESP. These two protocols provide data integrity, data origin authentication, and anti-replay service. These protocols can be used alone or in combination to provide the desired set of security services for the Internet Protocol (IP) layer.

The basic components of the IPsec security architecture are described in terms of the following functionalities:

- Security protocols for AH and ESP
- Security association for policy management and traffic processing
- Manual and automatic key management for the internet key exchange (IKE)
- Algorithms for authentication and encryption

The set of security services provided at the IP layer includes access control, data origin integrity, protection against replays, and confidentiality. The algorithm allows these sets to work independently without affecting other parts of the implementation. The IPsec implementation is operated in a host or security gateway environment giving protection to IP traffic.

Security token

Some online sites offer customers the ability to use a six-digit code which randomly changes every 30-60 seconds on a security token. The keys on the security token have built in mathematical computations and manipulate numbers based on the current time built into the device. This means that every thirty seconds there is only a certain array of numbers possible which would be correct to validate access to the online account. The website that the user is logging into would be made aware of that devices' serial number and would know the computation and correct time built into the device to verify that the number given is indeed one of the handful of six-digit numbers that works in that given 30-60 second cycle. After 30-60 seconds the device will present a new random six-digit number which can log into the website.

Electronic mail security (E-mail)

Background

Email messages are composed, delivered, and stored in a multiple step process, which starts with the message's composition. When the user finishes composing the message and sends it, the message is transformed into a standard format: an RFC 2822 formatted message. Afterwards, the message can be transmitted. Using a network connection, the mail client, referred to as a mail user agent (MUA), connects to a mail transfer agent (MTA) operating on the mail server. The mail client then provides the sender's identity to the server. Next, using the mail server commands, the client sends the recipient list to the mail server. The client then supplies the message. Once the mail server receives and processes the message, several events occur: recipient server identification, connection establishment, and message transmission. Using Domain Name System (DNS) services, the sender's mail server determines the mail server(s) for the recipient(s). Then, the server opens up a connection(s) to the recipient mail server(s) and sends the message employing a process similar to that used by the originating client, delivering the message to the recipient(s).

Pretty Good Privacy (PGP)

Pretty Good Privacy provides confidentiality by encrypting messages to be transmitted or data files to be stored using an encryption algorithm such Triple DES or CAST-128. Email messages can be protected by using cryptography in various ways, such as the following:

- Signing an email message to ensure its integrity and confirm the identity of its sender.
- Encrypting the body of an email message to ensure its confidentiality.
- Encrypting the communications between mail servers to protect the confidentiality of both message body and message header.

The first two methods, message signing and message body encryption, are often used together; however, encrypting the transmissions between mail servers is typically used only when two organizations want to protect emails regularly sent between each other. For example, the organizations could establish a virtual private network (VPN) to encrypt the communications between their mail servers over the Internet. Unlike methods that can only encrypt a message body, a VPN can encrypt entire messages, including email header information such as senders, recipients, and subjects. In some cases, organizations may need to protect header information. However, a VPN solution alone cannot provide a message signing mechanism, nor can it provide protection for email messages along the entire route from sender to recipient.

Multipurpose Internet Mail Extensions (MIME)

MIME transforms non-ASCII data at the sender's site to Network Virtual Terminal (NVT) ASCII data and delivers it to client's Simple Mail Transfer Protocol (SMTP) to be sent through the Internet. The server SMTP at the receiver's side receives the NVT ASCII data and delivers it to MIME to be transformed back to the original non-ASCII data.

Message Authentication Code

A Message authentication code (MAC) is a cryptography method that uses a secret key to encrypt a message. This method outputs a MAC value that can be decrypted by the receiver, using the same secret key used by the sender. The Message Authentication Code protects both a message's data integrity as well as its authenticity.

Firewalls

A firewall (computing) controls access between networks. It generally consists of gateways and filters which vary from one firewall to another. Firewalls also screen network traffic and are able to block traffic that is dangerous. Firewalls act as the intermediate server between SMTP and Hypertext Transfer Protocol (HTTP) connections.

Role of firewalls in web security

Firewalls impose restrictions on incoming and outgoing Network packets to and from private networks. Incoming or outgoing traffic must pass through the firewall; only authorized traffic is allowed to pass through it. Firewalls create checkpoints between an internal private network and the public Internet, also known as choke points(borrowed from the identical military term of a combat limiting geographical feature). Firewalls can create choke points based on IP source and TCP port number. They can also serve as the platform for IPsec. Using tunnel mode capability, firewall can be used to implement VPNs. Firewalls can also limit network

exposure by hiding the internal network system and information from the public Internet. Also, WE HAVE A LOT OF BIG WAYE to deal with it.

Types of firewalls

Packet filter

A packet filter is a first generation firewall that processes network traffic on a packet-by-packet basis. Its main job is to filter traffic from a remote IP host, so a router is needed to connect the internal network to the Internet. The router is known as a screening router, which screens packets leaving and entering the network.

Stateful packet inspection

In a stateful firewall the circuit-level gateway is a proxy server that operates at the network level of an Open Systems Interconnection (OSI) model and statically defines what traffic will be allowed. Circuit proxies will forward Network packets (formatted unit of data) containing a given port number, if the port is permitted by the algorithm. The main advantage of a proxy server is its ability to provide Network Address Translation (NAT), which can hide the user's IP address from the Internet, effectively protecting all internal information from the Internet.

Application-level gateway

An application-level firewall is a third generation firewall where a proxy server operates at the very top of the OSI model, the IP suite application level. A network packet is forwarded only if a connection is established using a known protocol. Application-level gateways are notable for analyzing entire messages rather than individual packets of data when the data are being sent or received.

Malicious software

Malware

A computer user can be tricked or forced into downloading software onto a computer that is of malicious intent. Such programs are known as malware and come in many forms, such as viruses, Trojan horses, spyware, and worms. Malicious software is sometimes used to form botnets.

Viruses

Computer Viruses are programs that can replicate their structures or effects by infecting other files or structures on a computer. The common use of a virus is to take over a computer to steal data.

Worms

Computer worms are programs that can replicate themselves throughout a computer network, performing malicious tasks throughout.

Trojan horse

A Trojan horse commonly known as a Trojan is a general term for malicious software that pretends to be harmless, so that a user willingly allows it to be downloaded onto the computer.

Ransomware and Scareware

Botnet

A botnet is a network of zombie computers that have been taken over by a robot or bot that performs large-scale malicious acts for the creator of the botnet.

Spyware

The term spyware refers to programs that surreptitiously monitor activity on a computer system and report that information to others without the user's consent.

Denial-of-service attack

A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of the concerted efforts to prevent an Internet site or service from functioning efficiently or at all, temporarily or indefinitely.

Browser choice

Web browser statistics tend to affect the amount a Web browser is exploited. For example, Internet Explorer 6, which used to own a majority of the Web browser market share, is considered extremely insecure because vulnerabilities were exploited due to its former popularity. Since browser choice is more evenly distributed (Internet Explorer at 28.5%,Firefox at 18.4%, Google Chrome at 40.8%, and so on) and vulnerabilities are exploited in many different browsers.

Application vulnerabilities

Applications used to access Internet resources may contain security vulnerabilities such as memory safety bugs or flawed authentication checks. The most severe of these bugs can give network attackers full control over the computer. Most security applications and suites are incapable of adequate defense against these kinds of attacks.

Internet security products

Antivirus

Antivirus programs and Internet security programs can protect a programmable device from malware by detecting and eliminating viruses; Before 2000 a user would pay for antivirus software, 10 years later however, computer users can choose from a host of free security applications on the Internet.

Security Suites

So called "security suites" were first offered for sale in 2003 (McAffee) and contain a suite of firewalls, anti-virus, anti-spyware and more.They may now offer theft protection, portable storage device safety check, private internet browsing, cloud anti-spam, a file shredder or make security-related decisions (answering popup windows) and several were free of charge as of at least 2012.

Outlook Express & Google+

Objectives : At the end of this lesson you shall be able to
- **explain outlook express**
- **explain Google+**

Microsoft Outlook

Microsoft Outlook is a personal information manager from Microsoft, available as a part of the Microsoft Officesuite.Although often used mainly as an email application, it also includes a calendar, task manager, contact manager,note taking, journal, and web browsing.It can be used as a stand-alone application, or can work with Microsoft Exchange Server and Microsoft SharePoint Server for multiple users in an organization, such as shared mailboxes and calendars, Exchange public folders, SharePoint lists, and meeting schedules. There are third-party add-on applications that integrate Outlook with devices such as BlackBerry mobile phones and with other software such as Office and Skypeinternet communication. Developers can also create their own custom software that works with Outlook and Office components using Microsoft Visual Studio. In addition, Windows Mobile devices can synchronize almost all Outlook data to Outlook Mobile.

Google+

Google+ (pronounced and sometimes written as Google Plus) is a social networking and identity service that is owned and operated by Google Inc. Google has described Google+ as a "social layer" that enhances many of its online properties, and that it is not simply a social networking website, but also an authorship tool that associates web-content directly with its owner/author. It is the second-largest social networking site in the world after Facebook. 540 million monthly active users are part of the Identity service site, by interacting socially with Google+'s enhanced properties, like Gmail, +1 button, and YouTube comments. In October 2013, Google counted 540 million active users who used at least one Google+ service, of which 300 million users are active in "the stream".

Creation

Google launched the Google+ service as an invitation-only "field test" on June 28, 2011, but soon suspended early invites due to an "insane demand" for new accounts. On August 6, each Google+ member had 150 invitations to give outuntil September 20, 2011, when Google+ opened to everyone 18 years of age or older without the need for an invitation. It was opened for a younger age group (13 years or older in US and most countries, 14 or older in South Korea and Spain, 16 or older in the Netherlands) on January 26, 2012. Google+ is available as a website and on mobile devices.

Before the launch, Google referred to Google+ as Google Circles, a name alluding to its emphasis on organising friendship information. Google+ is considered the company's fourth foray into social networking, following Google Buzz (launched 2010, retired in 2011), Google Friend Connect (launched 2008, retired by March 1, 2012) and Orkut (launched in 2004, as of 2013 operated entirely by subsidiary Google Brazil). Sources such as The New York Times have declared it Google's biggest attempt to rival the social network Facebook, which has over 1 billion users.