Internet and Web Designing --- Unit 1

Setting Up Email on Your Computer/ Configuring E-Mail Program

To setup your computer to send/receive email, you must already have the email account created in your Control Panel. You will need the following information when following the step by step instructions below for your email program.

Required Information

- **Username:** user@yourdomain.com (your full email address).
- **Password:** use whatever password you were assigned.
- **Incoming Mail Server:** Use mail.yourdomain.com (replacing yourdomain.com with your domain name).
  - Use SSL on port 993 (IMAP) or port 995 (POP)
- **Outgoing Mail Server:** Use mail.yourdomain.com (replacing yourdomain.com with your domain name).
  - Use SSL on port 465
  - "My outgoing (SMTP) server requires authentication" – **Yes**

Email is used for communicating by "mail" with other people on the Internet. There are many e-mail programs currently being used on the Internet, please note that our Customer Service Representatives are versed in using Outlook, Netscape Mail, and Internet Mail and may not have information on how to configure/use other E-mail programs.

When setting up your e-mail program(s), the following settings will most likely be used when configuring the program.

1. **Incoming (POP3) Server:**

   yourdomain.com (NOTE: DO NOT put 'www' or 'pop', etc. in front of the domain!)
2. **Outgoing (SMTP) Server:**

   yourdomain.com (NOTE: DO NOT put 'www' or 'smtp', etc. in front of the domain! The exception is with all Fully Managed Windows Servers, excluding the Business/Reseller III, you will need to use mail.yourdomain.com)**Some Internet Access Providers require you to use their SMTP server.
3. **POP3 account/user name:**

   Fully Managed Linux - youraccountname / Fully Managed Windows - youraccountname@yourdomain.com (This would be the name of the email account you created)
4. **POP3 account/user password:**

   This is the password for the POP email account that you have created.

Below is how to configure some of the popular client side email applications.

Netscape Mail

Open Netscape Browser

Go to Options menu bar and choose Mail and News

- Preferences
- Choose the Servers tab:
  1. Outgoing SMTP should be the mail server address of your dial-up company
  2. Incoming POP server should be yourdomain.xxx (substitute your domain name)
  3. POP3 username is the account you set up in your IMail Administration Page

     Click the Identity tab:
  4. Enter your name
  5. Enter your full e-mail address

6. Enter your reply e-mail address
7. Click Apply

Microsoft Office Outlook

1. Open Microsoft Office Outlook.

2. From the **File** menu, choose **Add Accounts...**.

3. Select the **Manually configure server settings** button, and click **Next** ...

4. Choose the **Internet Email** button.

5. Fill your information as follows...

6. On the right hand side, choose **More settings**...

7. Click the **My outgoing server (SMTP) requires authentication...**and make sure the **Use same settings as my incoming mail server** is selected**.**

••

Sending and Receiving Files with Email

One of the fundamental uses of email is to share photos and other files with friends, family, or colleagues.

In all of these options—Gmail, Yahoo! Mail, Hotmail, Outlook, and Mail—you'll want to keep an eye out for a a paperclip icon, the universal image for attachments in email programs.

The process is pretty much the same for all email programs:

- Open a new email message window, usually by clicking the "New Message" or "Compose Email" icon or the CTRL + N keyboard shortcut.
- Click on the menu item with a paperclip icon that says "Attach a file" or something similar (e.g., "Attach Files")
- Browse through your computer's folders and click to select the files/folders you want to attach. In most cases, you can select multiple files by holding down the CTRL key while clicking on each file.
- Click the "Open" or "Choose File" or another similar button to attach the file to your email.
- Then continue composing your email (put the email address of the person you want to send the attachment to in the To: field, add a subject and message in the body, and hit Send).

Using Files Attached to Email You Receive

When you receive a message that has files attached to it, you see the files in the body of the message. As when you send files in a message, you see the file's icon, name, and size. If the file can be displayed in the body, such as a TIFF or PDF, the contents of the file are displayed in the message. You can use the file attachments in the following ways:

- Select File, Save Attachments. Use the resulting sheet to move to a location and save the attachments.
- Click the Save All button at the top of the message. Use the resulting sheet to move to a location and save the attachments.
- If multiple files are attached, click the expansion triangle next to the attachment line in the message's header and work with each file individually.
- Double-click a file's icon to open it; drag a file's icon from the message onto a folder on the desktop to save it there.

- You can open the attachment's contextual menu and select one of the listed actions, such as Open Attachment, which opens it in its native application; Open With, which enables you to select the application in which you want the file to open; Save Attachment; or Save to Downloads folder, which saves the attachment in your designated Downloads folder.

Fighting spam

Spam is unsolicited email that may be delivered your address. It may contain advertising, “chain letters”, computer viruses, or even be a phishing attempt. Address databases are created by spammers using dedicated programs that pick addresses using a special dictionary or just collecting addresses posted publicly.

Unsolicited mail should be differentiated from honest mail. Proper mailing lists usually imply explicit consent. You can also unsubscribe to stop receiving such emails.

Yandex.Mail uses the “Anti-Spam” service, which learns from user-submitted spam complaints, to recognize spam. It puts suspicious email with spam features in the Spam folder.

Note: All messages in the Spam folder will be automatically deleted in 10 days. Note that you will not be able to recover deleted email.

Yandex.Mail filters not only incoming but also outgoing mail. Each email is checked for viruses. Messages in which a virus is detected will be rejected by the mail server and the sender will receive a report.

Electronic mail or Email is one of the easiest and most convenient channels where we can transfer information and share data with others. However, it is also common to receive information or emails that contain malicious attachments or dubious messages. Some email service providers filter and mark such dubious emails with the word “SPAM” in the subject of the email, indicating to the recipient that the email is either a junk email or unsolicited email with dubious content sent to numerous recipients by the sender. Clicking on links in such spam email may direct the recipient to phishing web sites or sites that download malware to the victim’s computer.
It is not surprising that most of us have encountered numerous spam emails in our inbox and believe it or not, your behavior online contributes to the spam messages that you receive. Here are five simple ways to fight spam and to protect yourself online:

1. Never give out or post your email address publicly

You should remember that everyone can easily access the Internet. That means, spammers are also lurking on the Internet and are constantly seeking available email addresses which they will send spam emails to. Posting your email address publicly allows others to send spam emails to you, or worse, hack your account if you are using a weak password.

2. Think before you click

There might be instances where your email service providers’ automated email filter mistakenly mark legitimate emails as spam email due to its content (e.g. the email contains a hyperlink). However, in most cases, emails marked as “SPAM” or redirected to the spam folder of your mailbox are sent by spammers. Subject of spam messages usually include offer of cheap prescription drugs, advertisements on new medicines, and status of packages from shipping companies. Make sure that you scrutinize the content of spam emails before opening any attachments (even if it looks like an innocent text or image file) or clicking on hyperlinks. Refrain from downloading contents blocked by your email service providers in such emails too.

3. Do not reply to spam messages

Almost all spam messages are malicious emails sent by unknown sources. These sources could be hackers who aim to hack into the computers of their victims. Never respond to spam messages because through this, the spammer will know that the email address is active and thus, it increases the chance of your email to be constantly targeted by the spammer.

4. Download spam filtering tools and anti-virus software

Spam filtering tools and anti-virus software can help to scan the emails that you received for malware. If the emails that you received contain malware, the malicious content would be quarantined and you would be prevented from opening it. This helps to alleviate the chance of emails containing malware from infecting your computer. As such, do select spam filtering tools and anti-virus software with such features to reduce your woes of having to decipher email contents.

5.Avoid using your personal or business email address

Do not use your personal or business email address when registering in any online contest or service such as applications, deal updates, etc. Many spammers watch these groups or emailing lists to harvest new email addresses.

There are many ways to avoid being a victim of spam messages. But the most important thing is to be cautious in opening your emails. Always make sure that the emails that you open are from trusted sources and do not look dubious.
****

Unlike real life battles with bladed and explosive weapons, the idea to fight spam is not very clear. Many competing tech companies are in the market to introduce the idea to fight spam in behalf of the users and the enterprise. We are not just here to fight spam, but to fight crime, as sending spam is a crime in many countries in the world. Many countries have legislated cybercrime laws, which always include criminalizing deliberate sending of mass junk email.

Spammers are not sending junk mails for the popularity - huge money motivates them. For every user click in their spam messages is a win for their wallets. Spammers will not take the effort of people to fight spam sitting down. They have started the retaliation of countering the action of many to fight spam, by deliberate misspellings of spam keywords. How many times we have seen spam words like Viagra misspelled? They have to do that in order to bypass the filters in their goal to counter our desire to fight spam.

Mainstream email clients like Microsoft Outlook and Mozilla Thunderbird have rudimentary engine that fight spam. It is through the use of "Junk folder", where the anti spam algorithm moves the spam email to the "Junk" quarantined location. The vulnerability of a built-in anti spam feature of the email clients is it is tied with the version. The newer the version, the more sophisticated the filter to fight spam is. Unfortunately, not everyone can upgrade to the next version as soon as it is available, especially in the enterprise setting where a strict upgrade cycle schedule is observed.

This situation can be fixed by installation of an anti spam system that fights spam using a special service hosted separately from the other servers. This is where Comodo, a leading name in privacy and security launched the Comodo Anti Spam Gateway. A total security solution for email spam. Comodo Anti Spam Gateway also covers protection for email attachments. This gives end-users and system administrator the confidence in opening email attachments, as it prevents malware by filtering them before the emails reach the user’s mailbox.

The prowess to fight spam can be empowered by Comodo Anti Spam Gateway. Its servers as a real time scanner, through its innovative Valkyrie anti spam engine. It fight spam from its source and blocks emails from known malicious domains from reaching the user's mailbox.

This filtering happens transparent to the user, and system administrators have a central control page. This is where they can granularly adjust the needs of the enterprise with regards to the aggressiveness of the anti spam solution.

Sorting Mail

Mail sorting refers to the methods by which postal systems determine how and where to route mail for delivery. Once accomplished by hand, mail sorting is now largely automated through the aid of specialized machines. The first widely adopted mail sorting machine was the Transorma, first made operational in Rotterdam in 1930.

Mail sorting systems are now also used by corporations and other mailers to presort mail prior to delivery in order to earn discounts on postage. In the United States, for example, presort discounts can reduce the cost of First-Class Mail from $0.42 to as low as $0.324. Many companies also use mail sorters to handle incoming mail such as checks, orders and correspondence. ☑

A method for sorting mail pieces for delivery by a carrier, wherein the mail pieces include both letters and flats, includes the steps of

a) sorting in a first sorting pass a batch of letters, each letter having a destination code thereon which corresponds to one of a predetermined number of delivery destinations for a carrier delivery route,

b) sorting in first sorting pass a batch of flats, each flat having a destination code thereon which corresponds to one of the predetermined number of delivery destinations for the carrier delivery route, using the same automated sorting machine which scans each delivery code and stores it in a computer memory;

c) sorting in a first sorting pass a batch of dividers having a scannable code thereon;

d) then sorting the letters, flats and dividers in at least one subsequent sorting pass, using the scanned and stored codes according to the computer-implemented sort scheme, resulting in a series of groups of mail pieces for each destination, which groups may include letters only, flats only, or both letters and flats, and which groups are in delivery route order, with a divider between each group.

E-Mail Mailing Lists

An **electronic mailing list** or **email list** is a special use of email that allows for widespread distribution of information to many Internet users. It is similar to a traditional mailing list – a list of names and addresses – as might be kept by an organization for sending publications to its members or customers, but typically refers to four things:

- a list of email addresses,
- the people ("subscribers") receiving mail at those addresses, thus defining a community gathered around a topic of interest.
- the publications (email messages) sent to those addresses, and
- a *reflector*, which is a single email address that, when designated as the recipient of a message, will send a copy of that message to all of the subscribers.

In order to send same email to a group of people, an electron list is created which is know as Mailing List. It is the list server which receives and distributes postings and automatically manages subscriptions.

Mailing list offers a forum, where users from all over the globe can answer questions and have them answered by others with shared interests.

Types of Mailing List

Following are the various types of mailing lists:

Response List

It contains the group of people who have responsed to an offer in some way. These people are the customers who have shown interest in specific product or service.

Compiled List

The compiled list is prepared by collecting information from various sources such as surveys, telemarketing etc.

Announcements

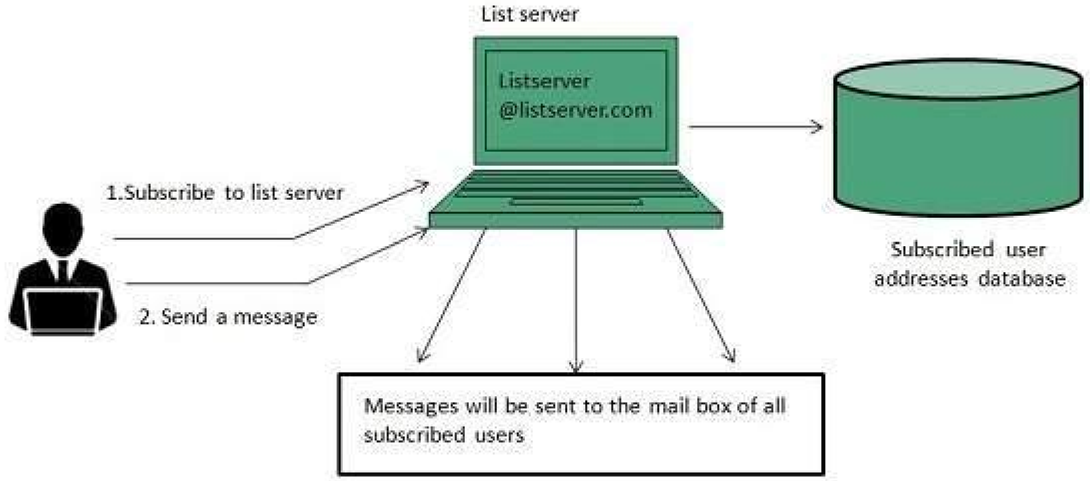
These lists are created for sending out coupans , new product announcements and other offers to the customers.

Discussion List

This list is created for sharing views on a specific topic suchas computer, environment , healt, education etc.

How does mailing list work?

Before joining a mailing list, it is mandatory to subscribe to it. Once you are subscribed, your message will be sent to all the persons who have subscribed to the list. Similarly if any subscriber posts a message, then it will be received by all subscribers of the list.



Finding Mailing List

There are a number of websites are available to maintain database of publically accessible mailing list. Some of these are:

- http://tile.net./lists
- http://lists.com
- http://topica.com
- http://isoft.com/lists/list-q.html

Mailing lists can also be found using Google website. In Google, move to directory and the follow: **Computers > Internet >Mailing List > Directories.**

Subscribing to Mailing List

To subscribe to a list, you need to send an email message to the administrative address mailing list containing one or more commands. For example, if you want to subscribe to Harry Potter list in gurus.com where name of the list server us Majordomo, then you have to send email to majordom@gurus.com containing the text, Subscribe harry potter in its body.

After sending the email, you will receive a confirmation email for your subscription. This email will include list of commands that will help you to perform various operations such as unsubscribing, receiving acknowledgement, and find out what list you are subscribed to.

••

Email Virus

An email virus consists of malicious code that is distributed in email messages, and it can be activated when a user clicks on a link in an email message, opens an email attachment or interacts in some other way with the infected email message.

Viruses and other malware distributed by email can wreak all kinds of havoc, including the following:

- the distribution and execution of ransomware attacks;
- enlisting the victim system into a botnet;
- crashing victim systems;
- providing remote access to victims' devices;
- theft of personal data or destruction of files on the victim storage media;
- creating unwanted pop-ups; and
- adding the victim system to a malvertisement

Email viruses often spread by causing the attachment or malicious message to be sent to everyone in the victim's address book.

Email viruses can be packaged and presented in a variety of different ways. Some can easily be spotted as malicious by virtue of subject lines that don't make sense, suspicious sender or other header fields and body content that looks off in some way. Other email messages containing malware can be more difficult for recipients to identify, as they reflect considerable effort by the malicious actor to make the email message appear to be sent from a trusted and known sender. This is particularly true for phishing attacks carried out to further business email compromise attacks.

Email viruses are often connected with phishing attacks in which hackers send out malicious email messages that look as if they are originated from legitimate sources, including the victim's bank, social media, internet search sites or even friends and co-workers. The attacker's goal, in these cases, is to trick users into revealing personal information, such as the victim's usernames, full names and addresses, passwords, Social Security numbers or payment card numbers.

Spam and malware-filled email messages are still considered to be one of the most effective means of social engineering used by hackers to spread and infect users with viruses and to attack the networks of their victims' companies.

Types of email viruses

Email viruses can take many different forms, and malicious actors work tirelessly to improve their malicious email messages and methods for email hacking, as well as the accompanying malware.

Email spam, also known as unwanted or unsolicited email, usually spreads malware through links in the message that lead to phishing websites or other sites hosting malware.

Virus hoax email messages, which contain a false warning about a nonexistent threat, are considered a form of socially engineered email virus or worm. Virus hoax messages may instruct the recipient to take some action, including forwarding the warning to all of their contacts. One variant of the virus hoax email builds on the tech support phone scam, in which a malicious actor attempts to engage the victim to defraud the victim.

Macro viruses are viruses written in a macro language used by other software programs, especially Microsoft Excel and Microsoft Word macros. Macro malware is transmitted through phishing email messages that contain malicious attachments, which contain the malicious macros.

Spambot programs are programs designed to harvest email addresses to build mailing lists for sending spam. While spambot programs are not usually distributed through email, they are instrumental in gathering valid email addresses to be used for the distribution of email viruses.

Examples of email viruses

Before always-on, broadband internet access was widely available, malicious actors depended on email to distribute their malware. While email viruses are still a common threat, they have been surpassed as a mass threat.

Melissa was one of the most notorious early email viruses. A fast-spreading macro virus, Melissa was distributed as an email attachment that disabled a number of safeguards in Word 97 or Word 2000 when it was opened by the victim. If the Microsoft Outlook email program was installed on a targeted system, Melissa re-sent the virus to the first 50 people in each of the victim's address books. Melissa was released into the wild in March 1999.

The fast-spreading ILOVEYOU virus surfaced on May 4, 2000, when it shut down email services in major enterprises, including the Ford Motor Company. The email virus carried the "I LOVE YOU" in the subject header, and it was estimated to have reached as many as 45 million users in one day.

The MyDoom email worm, released in January 2004, was the fastest-spreading email-based worm ever. MyDoom hit tech companies, including Microsoft and Google, with a distributed denial-of-service attack. Additionally, MyDoom spammed junk mail through infected computers, with text reading, "andy; I'm just doing my job, nothing personal, sorry." In 2004 it was estimated that 16% to 25% of all email messages had been infected by MyDoom.

The Storm Worm Trojan horse malware began spreading in January 2007 in email messages that exploited concern about European storms. The attackers initially spammed out hundreds of thousands of email messages, with a subject line reading, "230 dead as storm batters Europe." The malware infected the computers of users who opened the malicious attachment included with the email.

CryptoLocker ransomware, released in September 2013, was spread via email attachments. The ransomware encrypted victims' files. The attackers would send decryption keys to their victims in exchange for a sum of money. The primary means of infection was via phishing email messages containing malicious attachments.

Prevention

To prevent an email virus from infecting your client device or network, consider the following steps:

- Keep the mail client, web browser and operating system updated and patched.
- Use antivirus software.
- Don't open potentially dangerous attachments, such as PDF files, that have been included in email messages from unknown senders.
- Scan all attachments for malware.
- Don't click on links in email messages, and be careful of phishing email messages that appear to be from legitimate sources.
- Avoid opening any executable files included as email attachments. Attackers may try to disguise these files by naming them with two extensions, such as image.gif.exe, but .exe is the sign of an executable that will run automatically.

Prevention of email viruses is always preferable to removing them from infected systems. Using some sort of antivirus scanner, whether implemented in an enterprise firewall or in endpoint antivirus software, is always recommended.