

Syllabus 4.5 updates for Module 7

Disadvantages of E-Mail (7.4.1.2)

Although there are many advantages to e-mail, there are also some disadvantages. For example, attached files can spread viruses to your computer when opened or saved. An e-mail system can be insecure and leave you open to SPAM and Phishing (scam emails used to steal online identities). Unlike conventional mail, E-mail relies on power which can be a limitation during power failure. Size restrictions apply to attachments being sent over e-mail and space restrictions will limit what you can receive in your inbox. Restrictions on type of file attachments can limit what you send and receive over email. Web based mail accounts, although flexible and convenient, are limited in that some applications do not offer formatting options and, because a web mail account needs to be online to receive and send mail, you cannot read or compose your messages offline.

- Be very careful when opening file attachments - if you do not recognise the sender's address, delete the message immediately. NEVER open a file attachment with an .exe file extension.
- Ensure that your virus scanning software is set up to scan incoming and outgoing mail
- Always scan an attached file(s) for viruses before opening.
- Ensure that the size of the file attachment that you send via e-mail does not exceed the limit allocated to your account. Remember that the recipient of a message may not be able to receive mail over a certain size due to mailbox space limitations.
- Ensure that the recipient has the relevant application that will recognise and open the attached file.
- Some e-mail applications, such as Outlook and Outlook Express restrict certain file types from being sent/received via email. Database files (.mdb) are restricted files as are executable program files (.exe). This is to prevent possible virus infection. When you open an executable file, the program will run automatically; thereby spreading a potential virus to your hard drive.

Network Etiquette (7.4.1.3)

The development of the Internet has created a true global village, bringing together people with varying views, ideas and customs. In order that everyone can communicate without misunderstandings, a simple set of rules has emerged to form a convention for writing e-mails, known as **netiquette**. The netiquette protocol requires you to type a subject heading, keep the message brief and ensure that your spelling is correct. The writing style is informal. E-mails are personal and the expectation is that they will be dealt with by the addressee. When you receive an e-mail you are expected to either respond or acknowledge its receipt. However, this does not apply to unsolicited advertising or junk mail, often referred to as **spam**. Be careful how you word or type messages; typing in uppercase is considered SHOUTING, and using strong language is considered *Flaming* and can result in you being removed from newsgroups and forums. Many email applications offer text formatting tools, although some web based email systems do not have this option. When formatting text within an email message, be sensible in your choice of font, size and coloured backgrounds/images. Too many formatting features may detract from the message and appear unprofessional. Points to remember when formatting are:

- The formatting techniques that you use may not be readable on the recipient's computer
- Do not use uppercase to enter all of the text – use only for initial capitals
- Do not use inflammatory or strong language
- Keep fonts legible and ensure that you are using a default font that can be read by the recipient
- Keep font sizes sensible – no-one wants to scroll down a message to read a few words!

- Keep font colours legible – using light colours against a white background will be difficult to read.
- Ensure background colours and/or images do not increase the size of the message and do not detract from the content. Ensure that text is legible against coloured backgrounds.

2.2 Security Considerations

2.2.1 Guidelines and regulations (7.4.2.1)

Along with common business rules and regulations, there are guidelines regarding sensitive content, phishing and identity theft. **Phishing** refers to scam emails which attempt to gain your personal details, such as your login details, personal or bank details to gain access to your accounts or engage in other areas of identity theft. The email claims to come from an established company and may request you to visit a website where you are asked to enter personal details. NEVER click a hyperlink within an email message from an unknown source. The website address (URL) is often very similar to the genuine URL of the bank or other organisation that is being fraudulently represented. Be very careful about giving your details (account details, passwords, credit card details etc) over the Internet – your bank will never ask you to confirm account details, ID logons or passwords over email. Your ISP will not ask you to confirm your logon details or password over email. If you are unsure of the sender, delete the message immediately and contact the genuine company through phone or Internet, using their URL.

Sensitive content can be intercepted via email, so be very careful what you send. A digital signature verifies the sender of mail (see below) and encryption can be used to encode data in transit. Encoded data is called **cipher text** and the recipient requires a key to decode the encrypted file. Firewalls should also be used to prevent unauthorised access to your computer and prevent threats from viruses and other malicious content harming your computer and data. You should also maintain a good password protection policy, and change passwords regularly, never divulge logon details to a third party and also create user access rights if necessary to prevent unauthorised access to certain parts of the computer system. Large organisations should maintain a security policy which details the responsibilities of users regarding system and information security. The policy should set out reporting procedures in the event of a security breach. Some organisations expect employees to sign an Acceptable Use Agreement which sets out rules and guidelines for computer usage.

The Information Commissioner's Office is the UK's independent public body set up to promote access to official information and to protect personal information. Complaints relating to the Privacy and Electronic Communications Regulations 2003 (this covers unsolicited electronic marketing messages such as telephone, fax, email and text messages) are dealt with by this office. Visit their website on www.ico.gov.uk.

Saving a File Attachment (7.5.1.3)

Ensure that virus scanning software will scan both incoming and outgoing mail and also scan files that are downloaded from the Internet or received through email. The version of Outlook Express that you are using may not receive certain file types. Users of Outlook Express 6.0 may experience some difficulty in opening and saving file attachments if Internet Explorer 6.0 Service Pack 1 (SP1) or Windows XP SP1 is installed (both of which include Outlook Express 6.0). Outlook Express 6.0 blocks access to some attachments. You may find the Attach field missing from the message or the filename of the attached file unavailable when selected from the Preview Pane. Outlook Express will alert you to problems by displaying a message across the top of the email message with the following text: **OE removed access to the following unsafe attachments in your email: *name of file*.**

This problem occurs when the security setting to disallow potentially unsafe attachments to be saved or opened is disabled. You can check if this is enabled/disabled by selecting **Options** from the **Tools** menu, and then selecting the **Security** tab. You should only disable this option if you know and trust the source of the file attachment and you are satisfied that it is not a potential threat to your computer. It is recommended that this feature is turned back on once you have opened or saved the attachment.

If images are not displayed in a received message, check the setting for blocking images and other HTML content. You will need to turn this feature off if you want to view images or other external content in a HTML email.

Due to file type restrictions that the email server or system administrator (if on a network) has applied, you may not be able to view certain attachments, such as database files and program files. File attachments with the following file extensions: .vb or .vbs, .exe, .lnk, .bat should be viewed as a potential threat to your computer and should not be opened.

It is advisable to save a file attachment before opening it so that it can be scanned for viruses first.

A saved file can be scanned for viruses, using the anti-virus software that is installed on your computer. This can be performed by right clicking the file and choosing **Scan with...** (the name of your anti-virus software). The virus scanning software installed on your computer will detail any threats found and the actions that can be performed, such as quarantining, deleting or fixing the unsafe file.

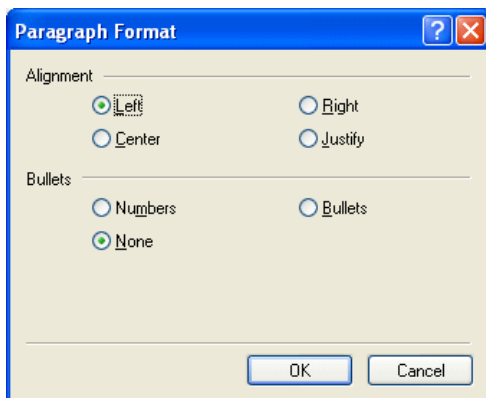
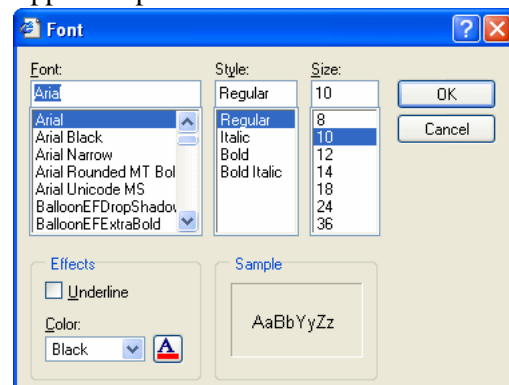
Creating a New Message (7.5.3.1, 7.5.3.2, 7.5.3.3 and 7.5.3.4)

Remember to conform to rules of netiquette when composing your email: keep the message brief, use a message subject, do not use capital letters or use inflammatory language, ensure that the text is free from spelling errors, ensure that fonts, sizes and colours are legible.

Formatting a New Message (7.5.3.1)

When using formatting tools and techniques to enhance an email message, you should consider how the email will be received. Are the fonts and sizes legible, do the font colours stand out against the background colour? Formatting should give the message a professional appearance and enhance readability. Formatted messages must be sent in HTML format. This option can be selected through selecting **Options** from the **Tools** menu, selecting **Send** and then selecting **HTML**. Please note that recipient may only be able to read the message as plain text. Only email programs that support MIME can read HTML formatting. If the recipient's program does not read HTML the message will appear as plain text with a HTML file attached.

- Highlight the text to be formatted and then select **Font** from the **Format** menu.
- From the **Font** dialog box, you have the option of changing the:
 - **font**
 - **style**
 - **size**
 - **effect**
 - **font colour**

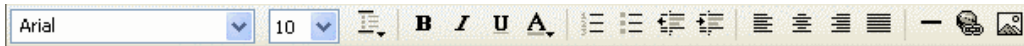


You can also change the layout:

- Select the relevant text within the message and then select **Paragraph** from the **Format** menu.
- From this dialog box you can change:
 - **Alignment** – left, right, centre, justify
 - **Bullets** – apply or remove
 - **Numbers** – apply or remove

Paragraph indents can be increased or decreased through selecting **Increase Indent** or **Decrease Indent** from the **Format** menu.

You can select any of the above formatting options from the **Formatting** toolbar:



Stationery can be applied to outgoing messages, but please note that the recipient may not be able to view any formatting applied to the message if their email program does not read HTML.

- Select **Apply Stationery** from the **Format** menu and choose a stationery item from the list
- Alternatively, select **More Stationery...** and choose an option

To apply formatting to **all** messages,

- Select **Options** from the **Tools** menu and then select the **Compose** tab.
- Select the **Font Styles** button for **Mail** and choose the font, size, style and colour for all outgoing mail.

Sending a Message with an Attachment (7.5.3.6)

There are certain measures that you should take before sending a file as an attachment.

- **Check the size of the file** before sending it. Ensure that it does not exceed the size limit allocated by your email server (more time will be taken to send the message and the size of file may eventually prevent the message from being sent) and also ensure that the recipient will be able to receive the file. The recipient may not be able to receive files over a specific size due to mailbox space limitations.
- **Check with the recipient** whether their email program has virus protection applied which blocks HTML graphics (Outlook Express has this setting). Certain file types, such as database files or program files (.exe) may also be restricted. Bear in mind that the recipient will need to have access to relevant software to be able to read certain files.
- **Check network restrictions** that may apply if the recipient's computer is connected to a network of computers at college or work. The system administrator/network manager may allocate a specific size limit that can be stored in the mail Inbox. If the attached file exceeds this amount, he recipient may not be able to download it. The network may also have restrictions applied regarding receiving certain file types.
- **Check virus protection restrictions** – these may prevent recipients from receiving file attachments, if they are also using Outlook Express. This program blocks pictures and Internet content from downloading on the computer, replacing the blocked object with a red x. The recipient will be bale to download legitimate content by selecting the banner that displays at the top of the message (the Info bar). These security features can be enabled/disabled:
 - Select **Options** from the **Tools** menu and then select the **Security** tab
 - Click the checkbox to either enable or disable the required option.

If there are problems sending large files, due to mailbox space limitations, you can send large messages as multiple smaller messages.

To do this :

- Select **Accounts** from the **Tools** menu and then select the **Mail** tab. Select the **Properties** button and then the **Advanced** tab. Check the box for **Break apart messages larger than** and enter the maximum size that your file server will allow.

If a recipient cannot view an inserted image that you have sent:

- Select **Options** from the **Tools** menu and then the **Send** tab.
- Click the **HTML Settings** button and then make sure that the **Send pictures with messages** ion is selected. Click OK twice.