

Microsoft Outlook 2010 – Level 1

1 – Email concepts



EMAIL CONCEPTS



Email provides a great way of communicating with friends, colleagues, business associates and the like. But with email comes certain responsibilities such as knowing how to protect yourself and others from viruses, understanding etiquette, dealing with spam and more.

In this booklet you will:

- ✓ gain an overview of how email works
- ✓ gain an understanding of email addresses
- ✓ gain an understanding of the benefits of email
- ✓ gain an understanding of general email etiquette
- ✓ gain an understanding of digital signatures

HOW EMAIL WORKS

Email is short for electronic mail and refers to a message sent from one computer to another. The computers may be in the same building and linked via a local

network, or they may be some distance apart and connected via the Internet and various telephone and communication systems.

Email Application

To send email from your computer you will need an email application (this is sometimes known as an **email client**). This application allows you to compose and send emails to other people, and to receive emails.

While there are a number of email applications on the market, the two most common are Microsoft Outlook which is supplied with Microsoft Office and Windows Mail which is available as a download from Windows 7.

This software needs to be installed on your computer.

Email Server

While an email client takes care of the business of writing and reading emails, it is the job of an **email server** to ensure that email is dispatched to the correct location and recipients.

Using normal mail (sometimes known as snail-mail) as an analogy, an email server is a bit like a post office. It takes the emails that you have created and sends them through the appropriate electronic pathways to the intended recipients. It also collects email messages that people are sending to you and it then delivers these emails to the email client on your computer.

If you send email messages to people in your company, these messages will generally only pass through one email server – the one that looks after the internal email in your business. This will most likely be something like Microsoft Exchange Server. When you send an email to a colleague outside your company, that email is sent to the server and the server then passes it to the email client on your colleague's computer – this is done in an instant.

When you send email via the Internet, however, the business of email servers becomes more complicated. Generally, it is your Internet Service Provider (ISP) who handles your Internet email, and, given the volume of mail they handle, they will have quite a few computers to do this. With Internet email there are separate servers that handle outgoing email (email that you are sending) and incoming email (email that someone is sending to you). Outgoing email is handled by the SMTP server (SMTP stands for Simple Mail Transfer Protocol), while incoming email is handled by the POP server (POP stands for Post Office Protocol).

To be able to send and receive emails via the Internet, computers need to be connected to both an SMTP and POP server. Therefore, when you send an email to someone via the Internet, it leaves your email client and goes to your ISP's SMTP server. From here it is sent to the recipient's POP server, which then passes it to your recipient's email client. Understanding that there is this alphabet soup of connections will help you to appreciate why emails sometimes get lost in cyberspace!

Email Account

To use an email server you will need to have an email account. An email account is a bit like having a post box at the local post office. An account is normally made up of two components: a user name which identifies you to other people and the system, and a password which ensures that other people can't access your mail.

With a proper user name (sometimes known as a user ID) and a password, your computer can connect to an email server.

EMAIL ADDRESSES

Just like your street address identifies where you live, you'll need to have an email address so that other people can send emails to you. Unlike street addresses, however, email addresses

comprise only a single line of characters. And the characters, once you understand what they mean, can tell you a great deal about the owner of the email address.

Identifying Email Addresses

An **email address** is a unique address on the Internet that allows people to send email messages to you.

An email address is written in a special way as follows:

username@domainname.topleveldomain.country

An example of an email address might be:

John.Jones@westsussex.gov.uk

The funny symbol in the middle (@) is known as an **at** symbol. If read aloud, the sample email address above would be spoken as "john at westsussex dot gov dot uk".

Note that email addresses are not case sensitive. But, in most locations the standard convention is to write email addresses in lowercase.

The User Name

The **user name** is used to identify the name of the owner of the email address. It is usually descriptive and pretty close to the actual name of the person. It could be just the first name, just the last name, both first and last names, first name plus the first letter of the person's last name, and so on. For example, John Smith may appear as: 'john', 'smith', 'johnsmith', 'johns', 'jsmith' and so on.

While there are no rules governing how the user name should appear, some workplaces have established a particular style that they want you to use. Your system administrator at work will probably set up your email address for you following company practice.

The Domain Name

The **domain name** helps the Internet identify the location of the email server that is hosting the email account. Sometimes, the domain name reflects the name of the Internet Service Provider (e.g. johns@bigpond.com) and other times it might be the name of your workplace (e.g. john@westsussex.gov.uk).

The Top Level Domain

The **top level domain** normally consists of three letters and identifies the type of organisation associated with the host's name. Examples of common top level domains include:

- .com** private or public company
- .gov** government department or organisation
- .edu** educational institution
- .net** networks usually reserved for Internet service providers
- .org** non-commercial organisations

The Country Identifier

Email addresses outside the United States are usually identified with an additional two letters at the end. Some of the more common ones are **au** for Australia, **uk** for United Kingdom, **nz** for New Zealand, **de** for Germany, **fr** for France, and so on.

THE BENEFITS OF EMAIL

There is little doubt that email has provided the greatest communication revolution since the invention of the printing press. With many people email has all but replaced the use of regular mail,

and billions of messages are sent every day. Email presents enormous benefits and advantages over traditional mail. Some of these are presented below.

It's Fast

With emails you can send a message to someone on the other side of the world literally within seconds. It is possible, therefore, to have an email 'conversation' where you are sending short messages back and forth with someone next door, in the next state or territory, or even on another continent.

It's Cheap

The cost of sending an email is normally made up of the time you spend online to send it. If you're sending lots of messages it makes sense to write them at a time when the computer is not connected to the Internet – this is technically known as **offline**. As you write these messages they can be 'Sent' in your email program – if the computer is offline the email program will keep these messages in a special Outbox until the computer is online. The messages will then be sent almost instantly. The cost of sending email therefore is usually much less than the cost of postage or even sending a fax.

It's Convenient – for lots of reasons

With email you can conveniently communicate with people who are either in different time zones, or who work and live differently to you. For example, you might send a letter to Aunty Flo at the time you work best (around 11:30 pm at night) knowing full well that Aunty Flo, who normally retires by 8:00 pm, will be able to log into her computer first thing in the morning to read your message. Or you might communicate with someone in a different country, even though it is past midnight in that country, and know that the recipient will open and read your message as soon as they log into their computer.

Email also prevents the game of telephone tag – where you ring someone but they are unavailable, and they ring you back when you are unavailable, so you return their call and they are again unavailable, and so on. With email you compose and send your message when it is convenient for you. Your recipient will open, read and respond to your message when it is convenient for them.

It's a fact that most busy people hate to get interrupted by phone calls. However, most busy people make a time to access and read their email. So with email it is much easier to get in touch with busy people.

You can also use email from a number of places. For example, let's say you're on a world trip. You can pop into an Internet café almost anywhere in the world and use one of the Web-based email services to send an email home to your friends and loved ones. You don't need to worry about stamps, local postage rates, or any of the other issues associated with mailing from another place.

It's Educational – maybe

Email is a form of communication done using the written word. In these times of television saturation there is evidence to suggest that email is bringing people back to writing and is thus increasing the levels of literacy in the community. The argument here is that email has brought back the art of letter writing, albeit it in a form that this is shortened, and lighter.

It Provides Access

Email is providing access to almost anyone in the world. In theory it is possible to send an email to the President of the United States, your favourite movie star or football player, and even Father Christmas. However, there is no guarantee that they will open and read your email.

It Provides A Record

Since outgoing messages are kept in the **Sent** box you'll always have a record of interactions with people with whom you have communicated. Although, if you are into major crime this may turn out to be a bad thing!

EMAIL ETIQUETTE

When you write and send an email there is a chance that it will live forever – a sobering thought when you sit down and really think about it. Therefore you should adopt courteous and polite habits when

writing your email messages. Quite a few guidelines have now been developed to help you be a good email citizen. Some of these are listed below.

Short Is Sweet

Reading text on the screen is harder (and arguably) more hazardous than reading on paper. Keep your emails short, sweet and to the point and your recipients will love you more.

Check Your Spelling

When you have composed your message spend a bit more time using the spell checker to check the spelling. Then re-read the message and ensure that the spell checker has done its job. You'd be amazed at how many online resumes have been sent straight to the **Deleted Items** folder because of bad and negligent spelling!

Make The Subject Line Meaningful

There's nothing more frustrating than receiving a message with a subject that contains 'Hi'. What does this mean? Is it going to waste my time? Always put meaningful text in the subject line of a message, such as "How about lunch?", "Sales Figures for June", and so on.

Watch What You Say

The way we interact with one another is done through a number of ways – we hear what is said and listen for inflections, and we see what people are doing with their eyes. In an email you can only really read what is being said – how do you know if it is serious or written in jest? When you compose an email, don't try to be too smart or cute, or you may find that your reader totally misinterprets what you are saying.

Avoid Flaming

Flaming is the act of telling somebody off using an email – and it should NEVER be done. If you have a gripe with someone, contact them over the phone or face to face, but never through an email. The big danger with email is that it can be read over and over again. If you use email to dress down someone they will read it once, then again, and again until they become enraged. And then they may flame you with an equally or even more vitriolic email. And guess what you'll do – yep, respond with yet another.

Don't SHOUT

In email shouting is done by using capital letters – and it has become almost as obnoxious to receive an email written in capital letters as it has for someone to come up and shout something in your ear. Don't use capital letters (except in the proper literary way for sentence starts, names, and the like) unless you specifically mean to shout something and be offensive.

Check The Attachments You Send For Viruses

Yeah, yeah, your recipient should really be responsible for this. But imagine how you'd feel if the potential customer you are trying to woo rings you up and says the email you sent had a virus. Wouldn't it be more professional and nice to be able to reply, "Gee, that's strange. I carefully checked and scanned the attachment(s) for viruses before I sent it. Are you sure the virus was from my email?"

Protect The Privacy of Others

When you want to send an email to a group of people you enclose their email addresses either in the **To** or the **Cc** fields. The problem here is that all of the recipients know exactly who else received this message, and, in many cases the address of each recipient is provided to all of the other recipients. If you are sending a message to many people and it is not necessary for the recipients to know who else received the message, put their addresses in the **Bcc** field and put your own address in the **To** field – Outlook needs to have at least one address in the **To** field.

EMAILS AND VIRUSES

A virus is a computer program that somehow or other manages to attach itself to an application on your computer with the intent of causing some mischief. Like human viruses the results can range from

virtually nothing at all, right through to, well, the death of your computer. In the past viruses have been passed along on floppy disks, but today the main transfer vehicle is email.

Types of Viruses

There are many types of viruses, the most common being: **boot sector viruses** that infect the start up program of your computer; **program viruses** that infect software programs on your computer; and **macro viruses** that infect macro programs written in Microsoft Word or Microsoft Excel. Within these types there are two broad categories: **Trojans**, which appear hidden and perform their nasty deeds without you noticing; and **Worms** which remain invisible, consume the resources on your computer, and appear only as your computer begins to slow down and choke up.

How Do You Get A Virus?

At the present time a virus is a program and it can only really be transmitted through other programs. Generally, there are three ways that a virus can get itself onto your computer:

1. From an infected disk or Flash drive that you place into the CD or USB drive. The virus here is transmitted usually through a hidden program that automatically loads when the disk is inserted.
2. From an attachment you receive via email and then (usually) double-click to open. Note, however, that some email viruses will launch without even being opened – they will launch when you view the infected message in the preview pane of your email software!)

The attachment may itself be a program or something like a letter that has a macro (program) in it that has been designed to automatically start as soon as the letter is opened.

3. From a software program that you download from a website. The software program (usually from a dubious source) will contain the virus which will infect your computer when the software is run.

How Do You Prevent Viruses From Infecting Your Computer?

The best way to protect your computer is by not having it connected to the Internet or any form of network, and to never place a disk into the CD drive. However, this is extremely impractical. Because you need to be connected in the real world, the best you can hope for is to minimise your risk of being infected.

To minimise the chances of being infected:

- Install, use and constantly update a good anti-virus software application on your computer, such as Nortons, Symantec, and the like.
- Install a firewall – this is special software that protects your computer from unwarranted entry from the Internet. Your company may already have a firewall set up.
- Set up the anti-virus software so that it runs in memory – this ensures that it is vigilantly and constantly checking incoming files for possible dangers and threats.
- *Always* use the anti-virus software to scan email attachments and NEVER open an attachment until it has been scanned and cleared.
- *Never* download software from dubious sources, such as screensavers, icons, freeware, and so on.

Note: At the time of writing it is not possible to get a virus by opening up a standard text-based email message. Viruses are only transmitted through email attachments. However, do not click on links in suspicious emails as these may take you to sites where your computer could get infected. With the sophistication of hackers and virus writers increasing daily, ensure that you check all of your incoming email very carefully!



DIGITAL SIGNATURES

While email and the Internet provide a cheap, convenient and very fast way of transmitting information, they are relatively easily accessed. One way to ensure that emails you send and receive

are secure is to use **digital signatures**. Digital signatures help to validate your identity and they can be used to sign important documents electronically.

About Digital Signatures And Digital IDs

Because some hackers send out email messages that appear to come from other people, it has become important for many people to verify that their incoming messages have actually come from known colleagues, clients or friends.

By using a **digital signature** you can prove to the recipient that the contents of the message were signed by you and not an imposter, and that the contents have not been altered in transit. Unlike a handwritten signature, a digital signature is hard to fake because it contains encrypted information that is unique to the signer and which is easily verified. When the recipient opens the message, the digital signature is validated and an icon will appear in the **Signed by** status line in the message header indicating the status of the signature –  shows that the signature is valid while  reveals that the signature is invalid.

Before you can send an email message containing a digital signature, you must first obtain a **digital ID**. Outlook enables you to do this from the **Trust Centre** (select **File > Options > Trust Centre** and then click on **[Trust Centre Settings]** and **E-mail Security**). From the **Trust Centre**, you can either import an existing digital ID from elsewhere (your employer may obtain one for you if you work in a large organisation) or you can obtain one from a third-party provider.

Digital IDs operate using a pair of keys: a **public key** and a **private key** – a key here is a bit like a pin number for a bank account. These keys are used for encrypting and decrypting data. If you use your digital signature to encrypt a message, you will need to export to the recipient a **certificate** that contains your public key (so that the recipient can add it to their address book and then Outlook can use this key to unravel or decrypt the information in the message) plus other information that the recipient's computer will need to validate your digital signature.

Adding a digital signature slows down the process of sending a message somewhat because your computer has to check with the computer that issued your digital ID to verify your signature. But because Outlook does check your digital ID, your recipient can be sure that your message really came from you – and that's the whole point of digital signatures.

CONCLUDING REMARKS

Congratulations!

You have now completed the **Email concepts** booklet. This booklet was designed to get you to the point where you can competently perform a variety of operations as listed in the objectives on page 2.

We have tried to build up your skills and knowledge by having you work through specific tasks. The step by step approach will serve as a reference for you when you need to repeat a task.

Where To From Here...

The following is a little advice about what to do next:

- Spend some time playing with what you have learnt. You should reinforce the skills that you have acquired and use some of the application's commands. This will test just how much of the concepts and features have stuck! Don't try a big task just yet if you can avoid it - small is a good way to start.
- Some aspects of the course may now be a little vague. Go over some of the points that you may be unclear about. Use the examples and exercises in these notes and have another go - these step-by-step notes were designed to help you in the classroom and in the work place!

Here are a few techniques and strategies that we've found handy for learning more about technology:

- visit CLD's e-learning zone on the Intranet
- read computer magazines - there are often useful articles about specific techniques
- if you have the skills and facilities, browse the Internet, specifically the technical pages of the application that you have just learnt
- take an interest in what your work colleagues have done and how they did it - we don't suggest that you plagiarise but you can certainly learn from the techniques of others
- if your software came with a manual (which is rare nowadays) spend a bit of time each day reading a few pages. Then try the techniques out straight away - over a period of time you'll learn a lot this way
- and of course, there are also more courses and booklets for you to work through
- finally, don't forget to contact CLD's IT Training Helpdesk on **01243-752100**