

# Microsoft Outlook 2010 – Level 1

7 – Junk email



# JUNK EMAIL

## InFocus

Some people love receiving junk mail such as catalogues, brochures, flyers, and the like in the post, while others hate it. Junk mail has now also become prevalent in email. Fortunately, Outlook has a **Junk Email** facility which allows you to take some control over unwanted and unsolicited email.

### In this session you will:

- ✓ gain an understanding of spamming and junk email
- ✓ gain an understanding of phishing junk emails
- ✓ gain an understanding of the junk email options
- ✓ learn how to add senders to the **Blocked Senders** list
- ✓ learn how to mark messages as safe
- ✓ learn how to manage the **Blocked** and **Safe Senders** lists
- ✓ learn how to import a **Blocked Senders** list
- ✓ learn how to export a **Blocked Senders** list
- ✓ learn how to review and delete junk email

# SPAMMING AND JUNK EMAIL

**Spamming** involves flooding the internet with many copies of the same email message on people who would not otherwise choose to receive it. Most spam

is commercial advertising, often for dubious products, get-rich-quick schemes or quasi-legal services.

---

## The Problem Of Spamming And Junk Email

While the occasional message promoting a product or service might be a nice diversion to an otherwise routine day, a constant barrage of these types of messages soon becomes a nuisance. Junk mail sent through the post presents a cost burden on the sender – brochures need to be printed and stamps need to be purchased. With junk email, however, there is virtually no cost to the sender as everything is generated and sent electronically. Over recent years marketers have discovered the benefits of being able to send hundreds of thousands of junk email messages, reaching a much greater market than could otherwise be achieved.

## The Difficulty Of Stopping Messages

The benefit, and ultimately the underlying flaw, with email is that once someone has your email address they can send you a message. Unless there are very elaborate checking points, known as **firewalls**, these messages eventually end up in your Inbox.

## How Outlook Helps Combat Unwanted Spam And Junk Email

- Since Outlook can't easily prevent junk email from getting to you, it can take appropriate action once the junk email arrives. At home when you receive an unwanted brochure in your letter box you can throw it straight into the rubbish bin. Outlook allows you to perform a similar act with your junk email. Since there are some consistent patterns associated with junk email, Outlook has included a built-in **Junk E-mail Filter** which it applies automatically to incoming messages. The filter doesn't single out a particular sender or type of message, but rather works on factors such as the content of the message and the time it was sent. Any messages that are caught in the filter are sent to the **Junk E-mail** folder where you can review and delete them.
- Spamming is a game of cut and thrust – spammers are constantly finding new ways around these filters. If you regularly receive unwanted email from a particular sender and cannot get the sender to stop, you can add the sender to the **Blocked Senders** list. Any mail from this sender or the sender's domain will then be deflected to the **Junk E-mail** folder. Conversely, you can also set up a **Safe Senders** list. Any mail received from these senders or the sender's domains will go directly to your Inbox even if the **Junk E-mail Filter** might otherwise catch them based on the content of the message.
- Junk email senders often send messages in HTML format which include pictures or sounds from an external source on the internet that act as a "**web beacon**". When you open one of these messages and the pictures or sounds automatically download, you are inadvertently verifying to the sender's server that your email address is valid. Your address can then be sold to spammers. To minimise this problem, Outlook blocks automatic picture downloads by default. If you're sure that the message is from a trustworthy source you can unblock the pictures or other external content.

## How Can We Help?

Help fight the war against spammers and junk email. NEVER purchase anything through junk email – it only encourages the spammers to continue their efforts. And, in many cases, you will find that your details have been passed onto other spammers for them to try their luck. Also, NEVER reply to spam messages. Even though you might be tempted to hurl virtual, electronic abuse at them, they are anonymous. By sending a reply you are confirming your existence to them and verifying that your email account is legitimate and viable!

# PHISHING AND JUNK EMAIL

Internet email scams are becoming increasingly common. An email scam involves sending emails to people falsely claiming to be a legitimate company with whom they commonly do business, such as

a bank, trying to get them to give out private information that will be used for identity theft. This type of email scam is also called **phishing**.

## How To Spot A Phishing Scam

An example of a common phishing scam would be if you received an email that appears to be from your bank requesting you to click on a hyperlink in the email so that you can verify your online banking information. Usually there will be a repercussion stated in the email if you don't follow the link, such as "your account will be closed or suspended". The goal of the sender is for you to disclose personal and/or account-related information.

Phishing emails can be tricky to identify because they commonly contain logos or other images taken from the website of the company mentioned in the scam email. They appear to be from a legitimate internet address. For example, the address in the **From** field in the email may be *lh@nab.com.au*. The clickable link in the email may also appear to be taking you to the company's website – for example, the hyperlink text may say something like "Log in to National Australia Bank" – but in fact, clicking on the link will take you to a spoof (or false) website.

## How Outlook Detects Phishing Messages

Because it can be hard to distinguish a phishing email message from a legitimate email message sent by, for example, your bank, the **Junk E-mail Filter** evaluates each incoming message to see if it is suspicious, contains suspicious links, or was sent from a spoofed email address.

Suspicious message detection is always turned on even if other junk email filtering is turned off. If the filter determines a message is both **spam** and **phishing**, the message is sent to the **Junk E-mail** folder, the message format is changed to plain text format, and the links in the message are disabled. In addition, the **Reply** and **Reply All** functionality is disabled and any attachments in the message are blocked.

If the **Junk E-mail Filter** does not consider a message to be **spam** but does consider it to be **phishing**, the message is left in the Inbox, but any links in the message are disabled and you cannot use the **Reply** and **Reply All** functionality. In addition, any attachments in the suspicious message are blocked.

## Common Phish Sense

Anyone with an email address is at risk of being phished. Any email address that has been made public on the internet (such as by posting in forums, newsgroups or on a website) is more susceptible to phishing as the email address can be saved by **spiders** that search the internet and grab as many email addresses as they can. This is why phishing is profitable for scammers; they can cheaply and easily access millions of valid email addresses to which they can send their scams.

The golden rule to avoid being phished is to **never, ever click on the links** within the text of the email. Always delete the email immediately. Once you have deleted the email then empty the **Deleted Items** folder immediately as well.

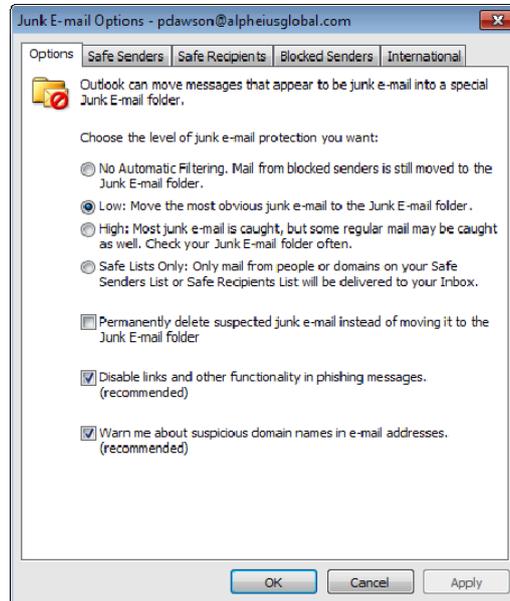
If, for some really odd reason you have this nagging feeling that this could just possibly be a legitimate email and nothing can convince you otherwise, you still need to adhere to the golden rule and not click on the link in the message. If you are still truly worried that an account may be in jeopardy if you do not verify your information, you need to open your web browser and type the URL to the website in the address field of your browser and log on to the website as you normally would (without going through the email link as the quick route). This will provide you with accurate information about your account and allow you to completely avoid the possibility of landing on a spoof website and giving your information to someone you shouldn't.

Now that you know how to avoid being phished, what should you do if you receive a phishing email message? Visit the website of the company from whom the email appears to be from and take the time to notify them of the suspicious email. Many companies do want to know if their company name is being used to scam people, and you'll find scam and spoof reporting links within some of these websites.

# UNDERSTANDING JUNK EMAIL OPTIONS

Because Outlook is a commonly-used email application, it tends to be a prime target of many spammers. As a consequence of this, Microsoft has created the **Junk E-mail Filter** in Outlook. While this filter is set up

with specific defaults, it is handy to understand the various options that are available to you so that you can best configure your system to cope with your own junk email problem.



## Junk Email Options

### **No Automatic Filtering**

Although this switches off the automatic **Junk E-mail Filtering** system, Outlook continues to check incoming mail by using the domain names and email addresses in your **Blocked Senders** list. Messages from these sources are still sent to the **Junk E-mail** folder.

Note: Phishing protection still works even if you turn off spam detection by selecting **No Automatic Filtering**.

### **Low**

A low level of filtering is performed on incoming mail. Use this option if you don't get many junk emails. (This is the default setting.)

### **High**

A high level of filtering is performed on incoming mail. Use this option if you frequently receive junk emails. Note that if you do select this option, you should regularly check your **Junk E-mail** folder as legitimate messages may be moved there accidentally.

### **Safe Lists Only**

Only messages from **Safe Senders** and **Safe Recipients** are allowed to pass into your Inbox. All other mail is treated as junk email. This is the most extreme form of protection.

### **Permanently delete suspected junk e-mail instead of moving it to the Junk e-mail folder**

This option permanently deletes suspected junk emails without sending them first to the **Junk E-mail** folder. Note that this option does NOT send the deleted messages to the **Deleted Items** folder.

### **Disable links and other functionality in phishing messages**

This option disables links and the **Reply** and **Reply All** functionality in phishing messages.

### **Warn me about suspicious domain names in e-mail addresses**

This option warns you when a domain name (@example.com.au) uses certain characters to make it appear to be a well-known brand or website. The intention is to trick you into thinking it is a legitimate email address when in fact it is spoofed.

# MARKING MESSAGES AS JUNK MAIL

While Outlook has its own **Junk E-mail Filter**, a lot of mail that is a nuisance to you will still get through to your Inbox. Outlook lets you allocate the senders of these messages to the **Blocked Senders**

list. Whenever future messages arrive from these people, the messages will automatically be sent to the **Junk E-mail** folder irrespective of whether they are picked up by the filter or not.

## Try This Yourself:

Open  
File

Before starting this exercise you **MUST** open the file *Watsonia\_10.pst...*

**1** Click on the **Inbox**  
There are two unread messages from companies that you've decided you no longer want to be bothered by...

**2** Click on the **FlightsFlights booking** message to select it

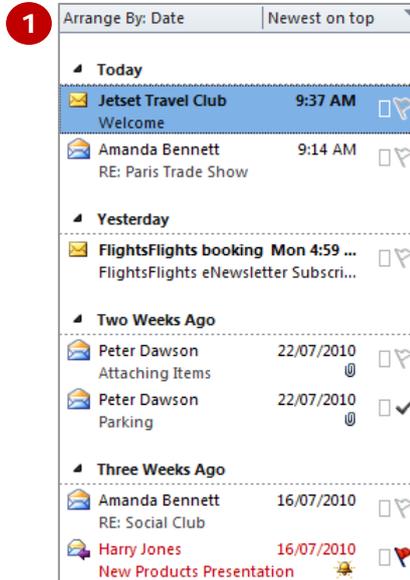
**3** Click on **Junk**  in the **Delete** group and select **Block Sender**

A message box may appear informing you that the sender has been added to the **Blocked Senders** list...

**4** Click on **[OK]** to close the message box

**5** Repeat steps **2** to **4** to add the **Jetset Travel Club** message to the **Block Senders** list

*Note: In this exercise we have marked two random messages for blocking. We are not inferring that the senders of these particular messages are involved in spamming. We have used these messages for illustrative purposes only*



## For Your Reference...

To **mark** a **message** as **junk email**:

1. Select the message in a message list
2. Click on **Junk**  in the **Delete** group on the **Home** tab
3. Select **Block Sender**

## Handy to Know...

- You can mark a message as junk email using the shortcut menu. To do this, right-click on the message and select **Junk > Block Sender**.

## MARKING MESSAGES AS SAFE

When the **Junk E-mail Filter** is active, there is a slight chance that particular messages that you know are from a safe source will still get picked up and sent to

the **Junk E-mail** folder. To avoid this, you can nominate specific senders or domains as being **safe** to ensure that future messages get through to your **Inbox**.

### Try This Yourself:

Same  
File

Continue using the previous file with this exercise, or open the file *Watsonia\_10.pst...*

1

Click on the **Junk E-mail** folder

The top message is actually from a person who you know to be trustworthy. Let's add this person to the **Safe Senders** list...

2

Ensure that the **'Pure greed' led spammer to...** message is selected, then click on **Junk**  and select **Never Block Sender**

A message box may appear informing you that the sender has been added to your **Safe Senders** list...

3

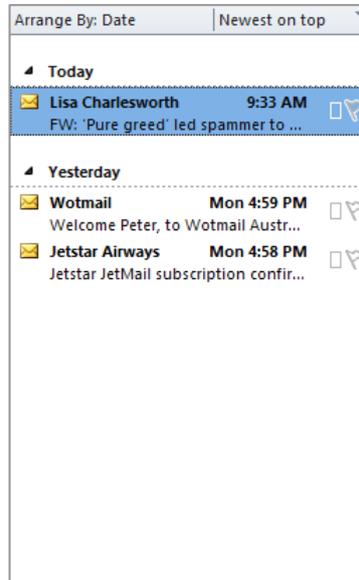
Click on **[OK]** to close the message box

Let's add a sender's domain name to the **Safe Senders** list. This will mean that all messages from that domain, irrespective of the author, will get past the **Junk E-mail Filter**...

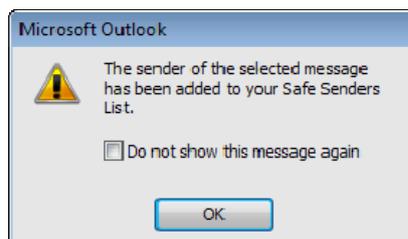
4

Click on **Junk**  and select **Never Block Sender's Domain**, then click on **[OK]** to close the message box if it appeared

1



2



If you want to avoid seeing potentially objectionable content in the **Junk**

**E-mail** folder, turn off the **Reading** pane in the **View** tab. Note that the **Reading** pane settings are unique for each folder.

### For Your Reference...

To **mark messages** as **safe**:

1. Select the message in a message list
2. Click on **Junk**  in the **Delete** group on the **Home** tab
3. Select **Never Block Sender**

### Handy to Know...

- You should regularly check your **Junk E-mail** folder. If you find a legitimate message there, you can click on **Junk**  and select **Not Junk**. This will move the message back to its original folder (usually the **Inbox**). You can then add the sender to the **Safe Senders** list if desired.

# MANAGING THE SENDERS LISTS

Outlook allows you to work directly with both the **Blocked Senders** and **Safe Senders** lists. When you work directly with these lists you can perform a variety of

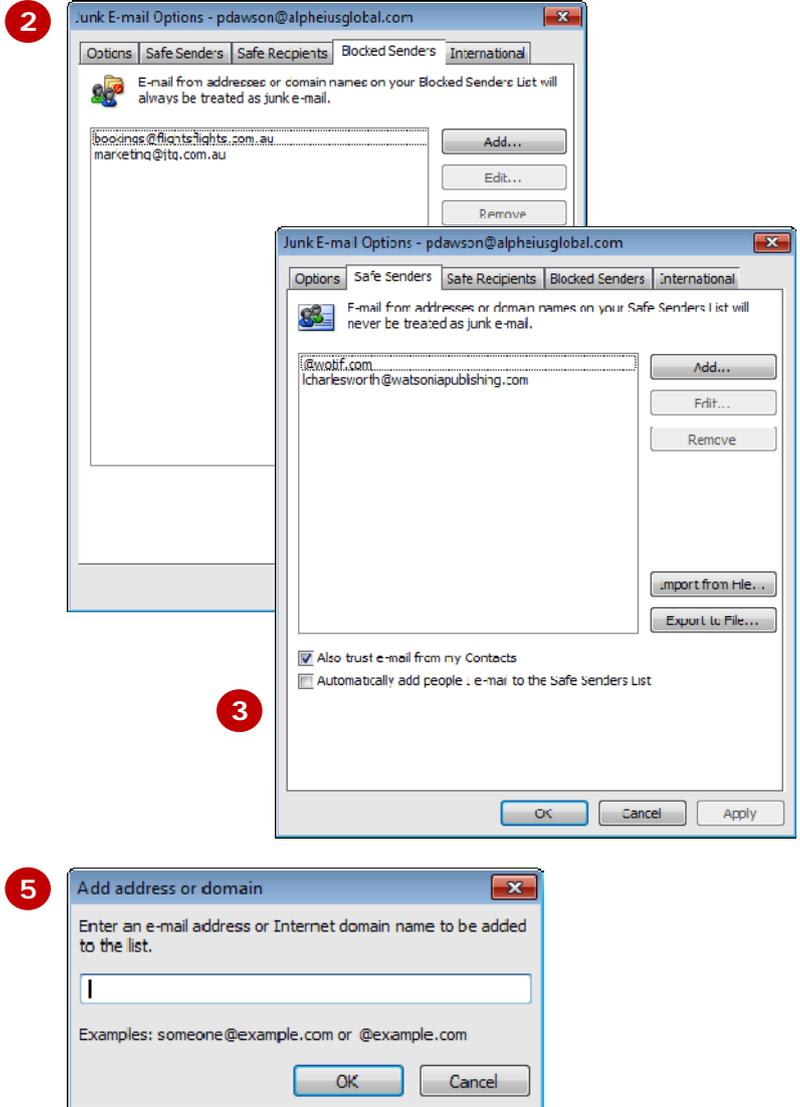
tasks, such as adding more senders to the lists, deleting entries from the lists, and even exporting copies of the lists for other people to use.

## Try This Yourself:

Same  
File

Continue using the previous file with this exercise, or open the file *Watsonia\_10.pst...*

- 1 Click on **Junk**  and select **Junk E-mail Options** to open the **Junk E-mail Options** dialog box
- 2 Click on the **Blocked Senders** tab to see the senders whose messages will be treated as junk mail
- 3 Click on the **Safe Senders** tab to see the senders that have been marked as being trustworthy
- 4 Click on **@wotif.com**, then click on **[Remove]** to remove this sender from the **Safe Senders** list  
*You can also manually add email addresses here...*
- 5 Click on **[Add]** to open the **Add address or domain** dialog box
- 6 Type **newsletters@travelonline.com** and click on **[OK]**
- 7 Click on **[OK]** to close the **Junk E-mail Options** dialog box



## For Your Reference...

To **work** with the **Senders Lists**:

1. Click on **Junk**  and select **Junk E-mail Options**
2. Click on either the **Blocked Senders** tab or the **Safe Senders** tab
3. Make the desired changes

## Handy to Know...

- You can manually add a domain name to the **Safe Senders** list. To do this, open the **Junk E-mail Options** dialog box, click on **[Add]** and type the domain name in the format **@domainname.com.au**.
- By default, messages arriving from your Contacts are treated as being trustworthy.

# IMPORTING A BLOCKED SENDERS LIST

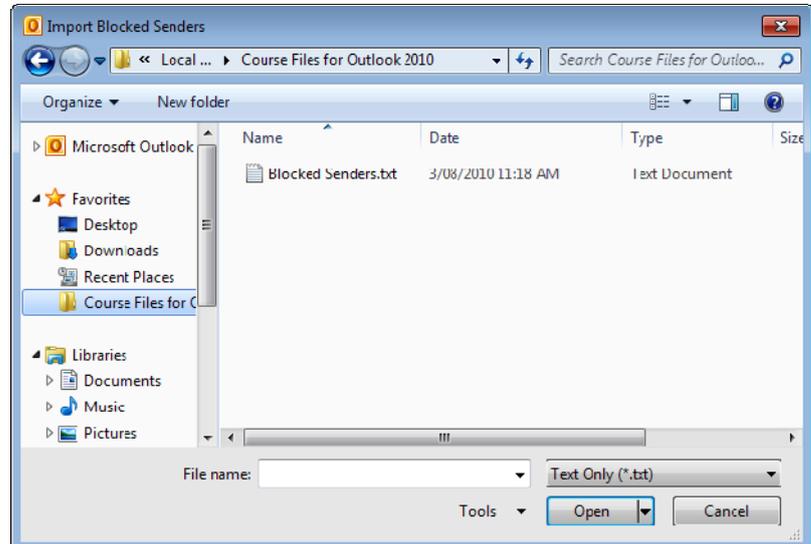
No-one likes to reinvent the wheel! There is a strong possibility that people who are sending junk email to you are sending them to other people as well. To help protect yourself from junk email you can

import a **Blocked Senders** list (which is also known as a **black list**) from someone else who has created one in their Outlook account.

## Try This Yourself:

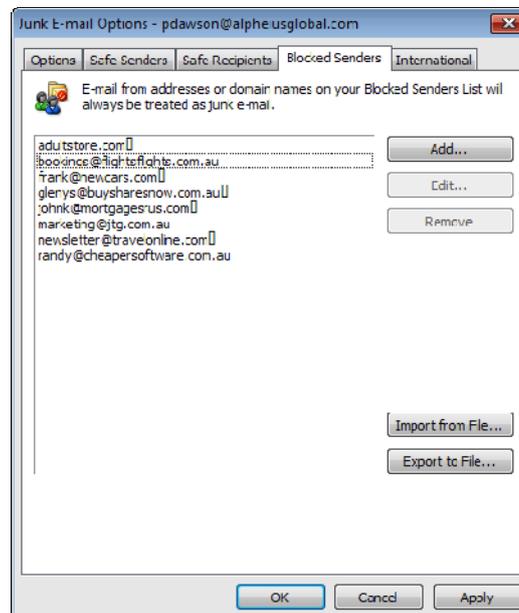
Same File

- 1 Continue using the previous file with this exercise, or open the file *Watsonia\_10.pst...*
- 1 Click on **Junk**  and select **Junk E-mail Options** to open the **Junk E-mail Options** dialog box, then click on the **Blocked Senders** tab
- 2 Click on **[Import from File]** to open the **Import Blocked Senders** dialog box, then navigate to the **Course Files for Outlook 2010** folder
- 3 Click on **Blocked Senders.txt** and click on **[Open]** to import the email addresses into your **Blocked Senders** list
- 4 Click on **[OK]** to close the **Junk E-mail Options** dialog box



2

3



## For Your Reference...

To **import** a **Blocked Senders List**:

1. Click on **Junk**  and select **Junk E-mail Options**
2. Click on the **Blocked Senders** tab
3. Click on **[Import from File]**
4. Double-click on the file, then click on **[OK]**

## Handy to Know...

- When you import a **Blocked Senders** list, any email addresses that appear in both **Blocked Senders** lists will be ignored during the importation process.

## EXPORTING A BLOCKED SENDERS LIST

Once you have gathered together a collection of blocked senders, you may wish to share this list with other computer users. You can do this by exporting your list to a relatively small text file using the

settings in the **Junk E-mail Options** dialog box. Other users can then import this text file into their own **Blocked Senders** list in Outlook.

### Try This Yourself:

Same  
File

1

Continue using the previous file with this exercise, or open the file *Watsonia\_10.pst...*

Click on **Junk**  and select **Junk E-mail Options** to open the **Junk E-mail Options** dialog box, then click on the **Blocked Senders** tab

2

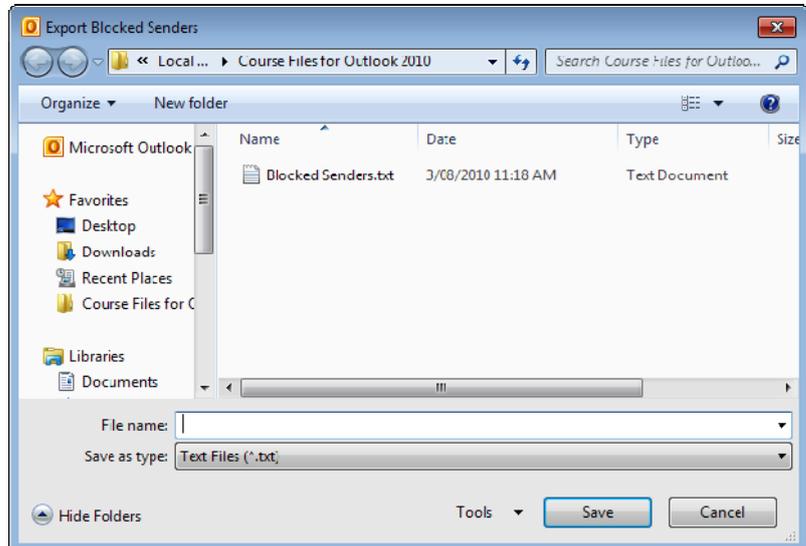
Click on **[Export to File]** to open the **Export Blocked Senders** dialog box, then ensure that the course files folder is open

3

Type **My Black List** in **File name**, then click on **[Save]**

4

Click on **[OK]** to close the **Junk E-mail Options** dialog box



2

### For Your Reference...

To **export** a **Blocked Senders List**:

1. Click on **Junk**  and select **Junk E-mail Options**
2. Click on the **Blocked Senders** tab
3. Click on **[Export to File]**
4. Name the file, and click on **[Save]** and **[OK]**

### Handy to Know...

- Exporting a **Blocked Senders** list creates a relatively small text file. This makes it easy to email the list to others as an attachment file.

## DELETING JUNK EMAIL

The **Junk E-mail Filter** automatically assesses incoming messages to determine whether or not they show junk email characteristics. All messages that appear to be junk email are moved to the **Junk E-**

**mail** folder. You should regularly review this folder and delete true junk messages and move to the correct folders any legitimate messages that were accidentally added.

### Try This Yourself:

*Continue using the previous file with this exercise...*

- 1 Click on **Junk E-mail** to see the messages in this folder

*All of these messages are junk emails so let's delete them...*

- 2 Click on the **Wotmail** message to select it and then press **Del** to delete it from the **Junk E-mail** folder

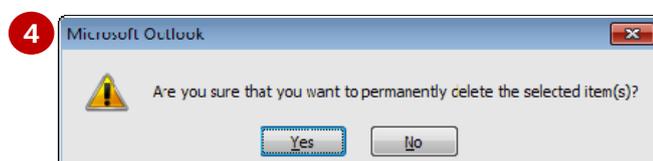
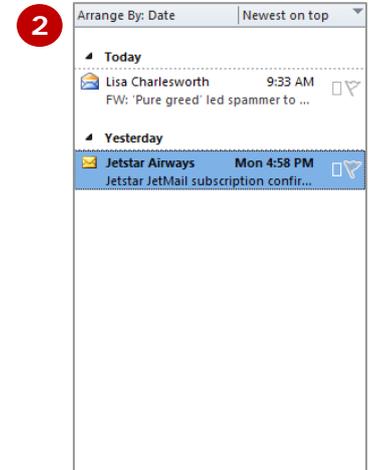
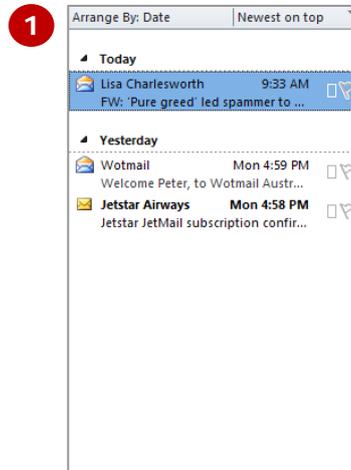
- 3 Click on **Deleted Items**  
*Notice that the Wotmail message has been moved to this folder. Let's permanently delete the remaining messages in the Junk E-mail folder...*

- 4 Click on **Junk E-mail**, select the two messages and press **Shift + Del**

*A message will appear asking you to confirm the deletions...*

- 5 Click on **[Yes]** to permanently delete the messages, then click on **Deleted Items**

*The two deleted messages will not appear in the Deleted Items folder as Outlook doesn't move permanently deleted messages to this folder*



### For Your Reference...

To **delete messages** in the **Junk E-mail** folder:

1. Click on **Junk E-mail**
2. Select the messages to be deleted
3. Press **Del** to move them to the **Deleted Items** folder, or Press **Shift + Del** to permanently delete them

### Handy to Know...

- You can quickly delete all items from the **Junk E-mail** folder in one go. To do this, click on the **Junk E-mail** folder and click on **Empty Folder**  on the **Folder** tab. Click on **[Yes]** to permanently delete the messages. Note that this option is available only for your default Outlook data file.

# CONCLUDING REMARKS

---

## Congratulations!

You have now completed the **Junk email** 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**