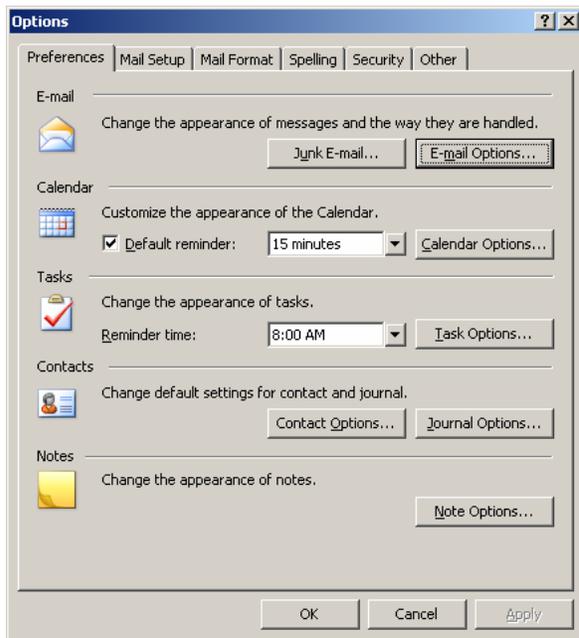


Microsoft Outlook 2003 - Security Tips

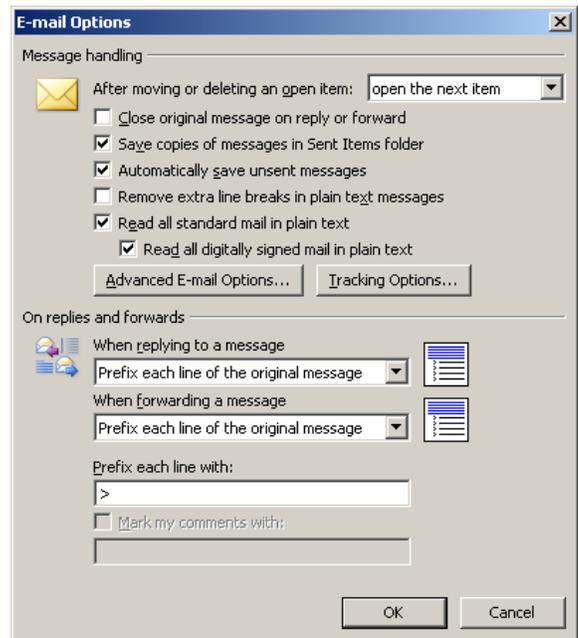
Note: This handout assumes you are running Windows XP Service Pack 2 and Office 2003 Service Pack 1

Read Mail in PLAIN-TEXT format

Reading mail in plain-text format prevents you from inadvertently executing harmful scripts which may be embedded in email messages. To read mail in plain-text format: Select the **Tools-Options** menu then select the **Preferences** tab, then follow the instructions in the figure below.



Click on the *E-mail Options* button



Check, *Read all standard mail in plain text*

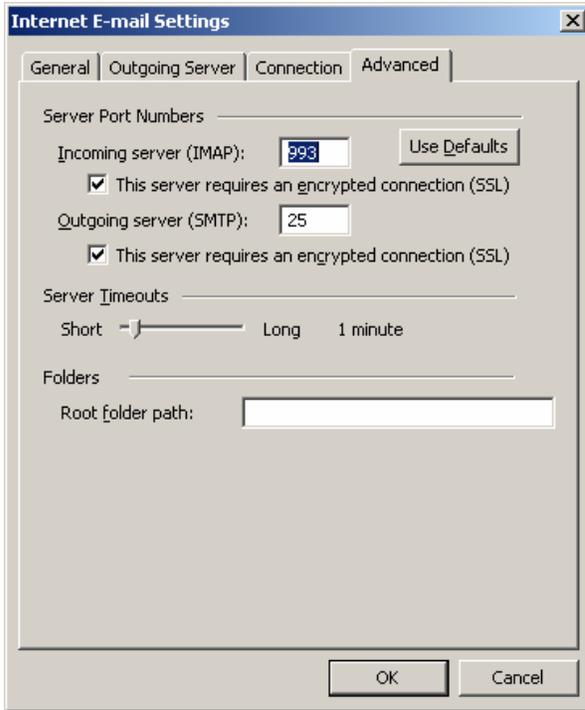
Operate Outlook 2003 in the Restricted Sites Zone

You should always operate Outlook 2003 in the restricted sites zone since this zone prevents potentially harmful content from executing. To select the Restricted Sites zone: Select the **Tools-Options** menu, then select the **Security** tab. Under Security Zones, set the zone to be **Restricted Sites**. Click **OK**.



Configure Outlook 2003 to use SSL

To avoid sending your email passwords over the network in clear-text format, you should configure Outlook 2003 to use SSL. Here's how: Select the **Tools-EmailAccounts** menu, then select **View or Change Existing Email Accounts** and click Next. Now, highlight your imapserver account and click the **Change** button then click the **More Settings** button and select the **Advanced** tab. For both incoming (IMAP) and outgoing (SMTP) servers, check the box titled **This server requires an encrypted connection**.



Outlook 2003 Attachment Security

Outlook 2003 has a decent automatic attachment filter; however you should still use the table below to help decide whether or not to open an attachment.

If the attachment is from someone you know AND the attachment is expected AND the attachment is work related AND the attachment is a document of a known probably safe type (Word-doc, Excel Spread Sheet ...)	Drag the attachment to a subfolder within your My Documents folder, right click on the copied attachment and perform a virus scan before opening it.
The attachment seems legit; but, is unexpected	Contact the sender before opening
The attachment is a joke file or other non-work related item.	Delete it.
The attachment is from someone you don't know	Delete it
The attachment is a program or script	In most cases, Delete it. If its work related, Contact the sender before opening

Outlook 2003 Macro Security

Select the **Tools-Macro-Security** menu; on the **Security Level** tab select either **High** or **Very High**.

