<u>Securing your emails</u>

The use of an email security certificate guarantees that people receiving emails from you will be confident that you actually sent them. This removes the possibility of third parties sending emails that purport to be from you.

By securing your emails you give confidence to the person receiving it that it 100% came from you.

When you receive emails then those that are digitally signed will have an envelope symbol on them. Here is one from Mozilla Thunderbird.
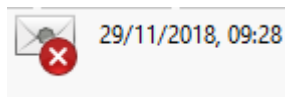

If you click on the envelope then it will give you further details.
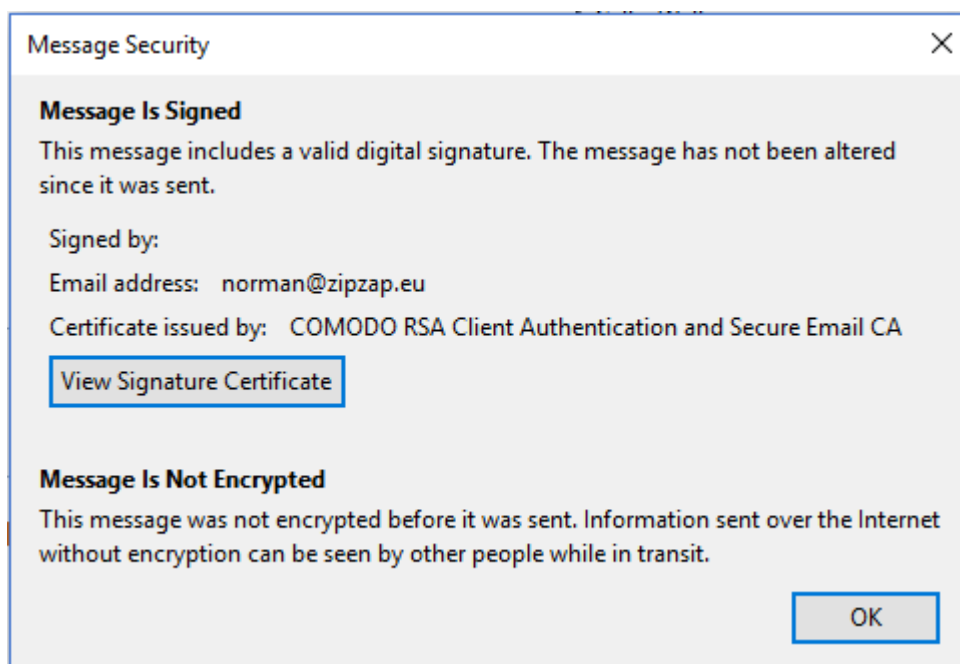
This says that the certificate is valid and from the correct sender.

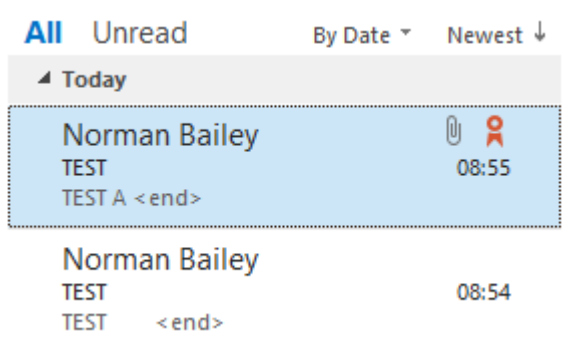If the certificate is invalid in any way then it displays like this.

If you click on the envelope then it will tell you what is wrong.

In this case the certificate is not valid because it is out of date.

Emails that have been tampered with will have a similar message.

Here's the same thing in Outlook :-

The top message is 'signed' and the one underneath is not.

You can buy email certificates at a low cost or you can get a free individual one from Comodo here :–

https://www.instantssl.com/ssl-certificate-products/free-email-certificate.html

Please note that you should set your default browser to Internet Explorer or Firefox while you obtain the certificate as it checks and locks the browser validity in the reply. So, you must use the same browser to apply for and receive the email certificate. Afterwards, if you changed it then you should change it back.

You cannot use Chrome or Edge to get the certificate at all.

If everyone used secure emails then the problem of spam and scams would go away.