Tech Tip for ensuring URL's are bona fide.

This is useful when you receive suspicious emails or websites, and you wish to check the authenticity of the website link(URL).

With the email or website open, you can view the URL before selecting the link.

To do this in:

- With products that have a mouse, you hover the mouse over the URL and the URL appears in a popup with the full address.
- With touch screen devices you continue to apply pressure on the URL until it appears in a popup with the full address.

In the below diagram (which I have intentionally hazed out the phony email address) you can see that the provided email address has a different address to the send email. Jewel Foster is not the recipient.

Things to look for before selecting the link:

1. Do you know the person or website; if not become suspicious.
2. The content has spelling mistakes, or has poor, nonsensical grammar.
3. The link does not match the popup.
4. The email or web address is incorrect, or you are unfamiliar with domain identification.
5. The content is not something that you are interested in Viagra, Somali prince, lost inheritance, or a Russian bride.
6. Your antivirus software, or your computer, is warning you about the content.

You should then just delete the content, and the recommended way is to use the <delete> key on your key board. Not all presented graphics on the screen will function as portrayed. For example, a delete or close graphic may in fact do something entirely different.

If you receive continual correspondence, you will need to implement an antivirus, spam filter, or malware software.   If you already have this in place, the settings need to change to provide additional protection. If you are in doubt about this, then you should contact your IT provider; they will know what to do.