HOW DO I SPOT PHISHING EMAILS?

Three steps for being well prepared

Verify the sender.

Are the sender and subject of the email plausible in this context?

You should look very carefully at the sender's email address in particular, as the domain can be faked to appear deceptively genuine.

Be skeptical. If you have any doubts before you open the email, use another channel to double-check with the sender that they sent it.

Check the target domain before clicking any links.

Hover the mouse over the link and pay attention to the part before the third slash "/"

Here's a quick example:

https://www.google.com/services
takes you to Google

https://www.google.com.myaccounts.biz/services
takes you to the URL of myaccounts.biz

Be careful with attachments.

Particular care is needed where emails have attachments.

Do not enable edit mode for external documents.

This could allow malware to be downloaded, infecting your computer and the network.

HORNETSECURITY