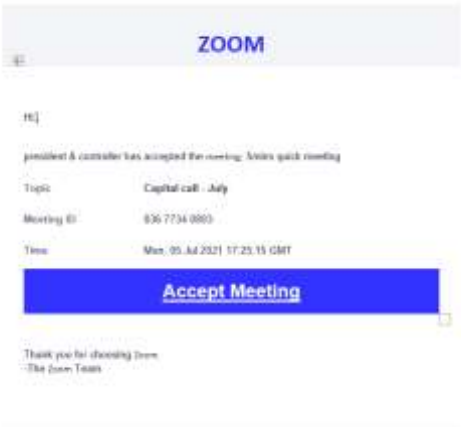
'CYBER AWARE' – PHISHING

We are seeing a significant increase in phishing attacks – these take the form of fake emails designed to make you click on a link that either tempts you to provide personal information, or allows malware to be downloaded.

Two recent examples are shown below, these referenced common types of applications that are regularly used due to the challenges of working through a pandemic. This familiarity is often used to convince staff that the email is genuine.



All staff should be vigilant for these types of emails, and in the event of receiving something suspicious, do not open or click on any links, but forward to DL-spamblocker@belfasttrust.hscni.net

5 WAYS TO SPOT A FAKE EMAIL

NO PERSONALISATION

Does it have a generic greeting?
Is there a lack of contact information for the sender?

UNEXPECTED

Is it from a stranger, or from an email address not normally used by the sender,
And is it offering something too good to be true?

SPELLING & GRAMMAR ERRORS

Does it contain any spelling or grammar mistakes?
Does it have spelling normally used by a non-UK dictionary?

PERSONAL INFORMATION REQUESTS

Is it asking for personal information, bank details or passwords?
Does it have a link to external websites asking for personal details?

HIGH URGENCY OR THREAT

Does it have a sense of urgency?
Does it have an uncharacteristic deadline, or is it
threatening or a threat implied?