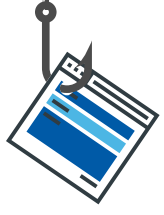
CYBER SECURITY

INCREASED EXPOSURE TO PHISHING THREATS

TYSERS

LOOK OUT FOR EMAILS...

...that appear to be from organisations such as the PHE (Public Health England), or the WHO (World Health Organisation). Scammers create emails that appear to come from these sources, but contain malicious phishing links or dangerous attachments.



BE CAUTIOUS WITH EMAILS...

...asking for charity donations for health studies, doctors, or victims that have been affected by the Coronavirus (COVID-19). Scammers often create fake charity emails after global events.

DON'T PROVIDE CREDIT CARD DETAILS...

...unless you are visiting a trusted website, e.g. amazon.co.uk, and see a little padlock in the address bar to indicate the site is secure.

IT'S NOT JUST EMAILS...

...phishing is not limited to email only. Text messages are also being sent, for example, claiming that the recipient will be entitled to receive a payment from the Government.

5 SIMPLE TIPS TO AVOID GETTING TRICKED

BEWARE OF ONLINE REQUESTS FOR PERSONAL INFORMATION

A coronavirus-themed email that seeks personal information like your National Insurance number or login information is a phishing scam. Legitimate government agencies won't ask for that information. Never respond to the email with your personal data.

CHECK THE EMAIL ADDRESS OR LINK

You can inspect a link by hovering your mouse button over the URL to see where it leads. Sometimes, it's obvious the web address is not legitimate. But keep in mind Phishers can create links that closely resemble legitimate addresses. Delete the email.

WATCH FOR SPELLING & GRAMMATICAL MISTAKES

If an email includes spelling, punctuation, and grammar errors, it's likely a sign you've received a phishing email. Delete it.

LOOK FOR GENERIC GREETINGS

Phishing emails are unlikely to use your name. Greetings like "Dear sir or madam" signal an email is not legitimate.

AVOID EMAILS THAT INSIST YOU ACT NOW

Phishing emails often try to create a sense of urgency or demand immediate action. The goal is to get you to click on a link and provide personal information - right now. Instead, delete the message.

Ensure you and your employees don't fall victim to Cyber Criminals – your business could lose a lot of money.

To protect against financial losses speak to your insurance adviser about Cyber and Crime Insurance protection.

TO LEARN MORE ABOUT CYBER & CRIME INSURANCE PROTECTION **CLICK HERE**