SOUTH WEST POLICE
RCCU
Regional Cyber Crime Unit

Phishing Guidance

Phishing is the use of deception and social engineering by criminals to fraudulently gain private/ financial information, or distribute malicious software. This is commonly done by tricking individuals into believing that a fake email, text message, or website is from a trustworthy company or person.

Phishing emails and text messages (SMS)

Phishing emails are sent by criminals to large numbers of random people (**phishing**), or can be targeted at you/your organisation/your team (**spear phishing**).

Phishing emails often contain speling mistakes or grammatical errors that an email from a professional company or organisation wouldn't normally contain.

Never rush into acting upon an email. Stop..... and read with a critical eye, and question the source if not convinced it's genuine.

Phishing only works if you allow yourself to be rushed into replying or clicking on a link in the email or message.

STOP and **THINK** before replying or clicking on anything.

Coronavirus pandemic and phishing scams

Cyber criminals are exploiting anxiety and concern during the coronavirus pandemic. These phishing scams are using new means of exploitation related to the novel virus, including:

- Pretending to be an official from the World Health Organisation (WHO) or other health authority with links to "Health Advice"
- Pretending to be an official email from HM Revenue and Customs with the false promise of a tax refund with a link to a "Tax rebate"
- Scamming for money in online "fundraising" that is not related to an official charity

These fraudulent emails or messages may have an official looking badge and other details, however, clicking any links could result in downloading malicious software or opening a fraudulent webpage.

Fear and misinformation is central to the success of COVID-19 phishing scams, and they should be treated the same as any email:

STOP and **THINK** before clicking on anything.

What should I do if I think I have received a suspicious message from an individual?

An email, text message or phone call from an individual may be suspicious if it's unexpected, or you're being asked to do something you normally wouldn't do and there are other procedures in place to complete that task (such as providing bank details or personal details to HR). If suspicious you should:

- Telephone or contact the sender through other means, using contact details that confirm the sender's identity and are **NOT in the original email or message**
- Contact HR or your line manager to confirm the request, if it is a work email
- Not be pressured into acting on a request before you have confirmed it is legitimate

What should I do if I think I have received a suspicious message from a company or bank?

A fraudulent email or text message will try and get you to follow a link to a phishing website which has been disguised to look exactly like a legitimate website such as PayPal or your online bank. If suspicious, you should:

- Close the email without clicking on any links
- Open a web browser and visit the legitimate website - don't use the web address in the suspicious email
- Log into your account using your credentials as normal. If there really is a reason why the company wanted you to log in, then a message will be waiting for you confirming this

How else can I protect myself from Phishing?

- Update all of your devices and apps to the latest versions regularly
- Ensure that you have an antivirus - make sure that it's switched on and receiving updates
- Switch on your firewalls (this should never be disabled)
- Always check that you have a secure connection when accessing a website - look that you've entered the website address correctly, and that the connection is encrypted (**https://** - click the padlock in the browser bar)

If you identify a phishing email or attempt, then report it to the NCSC's Suspicious Email Reporting Service (SERS) at (https://www.ncsc.gov.uk/information/report-suspicious-emails), or to the relevant lead in your organisation.