New Phishing Scam Reporting Tool Launched

Report / forward phishing email scams to: report@phishing.gov.uk

The National Cyber Security Centre has announced the launch of a central email address which can be used to report phishing email scams.

Phishing email scams have been around for a very long time, but the fraudsters who send them often use current events such as COVID-19 to make them appear genuine.

Latest phishing COVID-19 phishing scams include:

- Emails that encourage recipients to provide their bank details in order to receive coronavirus related Government payments, including scam HMRC job retention emails

- Emails designed to look like they have been sent from the NHS or other Government bodies. These emails might falsely claim to link to a list of coronavirus cases in your area

- Emails that offer purported medical advice, tests or treatments to help protect you against the coronavirus.

- Emails targeted at businesses and specifically those working from home. These scam emails may appear to come from the company IT department or personnel department and contain fake policy document attachments which the recipient is asked to download and read

- Scammers are also seeking to exploit the increasing use of online communication platforms such as Zoom and Microsoft teams by sending out phishing emails carrying these platforms names.

Phishing emails sent by scammers will typically contain links to scam websites or virus laden attachments. Following links in suspicious emails or opening or downloading attachments may increase the recipient's exposure to malicious websites, computer viruses, spamware and ransomware.

IT IS BEST TO TRY TO AVOID Downloading or Opening Attachments or Clicking Links in a suspicious email. **Simply forward the email to report@phishing.gov.uk**

Just use the [Forward] option in your email application to send the email to report@phishing.gov.uk

If a scam email purports to be from your bank, your bank may also have its own phishing email address too, so you could also copy it to your bank as well to alert your bank directly.

& once you have forwarded a suspicious email delete it from your device!

The National Cyber Security Centre say:
If we discover activity that we believe is malicious, we may:
• seek to block the address the email came from, so it can no longer send emails
• work with hosting companies to remove links to malicious websites
• raise awareness of commonly reported suspicious emails and methods used (via partners).
Whilst the NCSC is unable to inform people reporting phishing emails, of the outcome of its review, it has confirmed that it does act upon every message received.

If you require telephone advice or support in relation to scams, please phone the Citizens Advice Consumer Service on 0808 223 1133.

They will also alert Warwickshire Trading Standards Service who can provide additional advice.

Keep up to date on the latest scams: https://www.warwickshire.gov.uk/scams