In response to COVID-19, many members will be encouraging staff to work from home. This presents new cyber security challenges that must be managed.

For many organisations, home working has become the new normal. Remote technology offers huge benefits, but can open employees up to increasing frequent and sophisticated online scams.

As a result of the COVID-19 situation, cyber criminals are using a range of new techniques online to trick people into handing over money or reveal sensitive information (phishing). Example scams include the sale of medical supplies, fines for irresponsible behaviour, notifications of tax rebates and encouraging people to donate money to vaccine research or fake charities.

Additionally, without the benefit of an office environment and colleagues to consult, it can be more difficult to make a sensible judgement on a received communication.

This guidance:

1. Recommends steps to take to prevent cyber scams
2. Provides some tips on how individuals can spot the typical signs of phishing emails
3. Identifies sources of further information and training

---

1. Recommended steps to take to prevent cyber scams

a. Communicate the basics to employees

Encourage staff to be particularly vigilant at this time. Following the below steps, suggested by Government, can help to ensure staff are alert to the dangers posed, particularly by emails.

- **Stop:** Taking a moment to stop and think before parting with your money or information could keep you safe
- **Challenge**: Could it be fake? It's ok to reject, refuse or ignore any requests. Only criminals will try to rush or panic you
- **Protect**: Contact your bank immediately if you think you've fallen for a scam and report it to Action Fraud

b. Find out more and upskill

Visit the UK's National Cyber Security Centre's website (www.ncsc.gov.uk) for help and advice. They have many free resources, including:

- For employers: Secure Home Working Guidance https://www.ncsc.gov.uk/guidance/home-working
- For employees: Guide to Spotting and Dealing with Phishing Emails https://www.ncsc.gov.uk/guidance/suspicious-email-actions

The NCSC also offer a free, 30-minute online training package:

- Stay Safe Online: Top Tips for Staff https://www.ncsc.gov.uk/blog-post/ncsc-cyber-security-training-for-staff-now-available

2. How individuals can spot the typical signs of phishing emails

Here's some tips on spotting phishing emails:

- Many phishing emails have poor grammar, punctuation and spelling
- Is the design and overall quality what you'd expect from the organisation the email is supposed to come from?
- Is it addressed to you by name, or does it refer to 'valued customer', or 'friend', or 'colleague'? This can be a sign that the sender does not actually know you, and that it is part of a phishing scam
- Does the email contain a veiled threat that asks you to act urgently? Be suspicious of words like 'send these details within 24 hours' or 'you have been a victim of crime, click here immediately'
- Look at the sender's name. Does it sound legitimate, or is it trying to mimic an organisation or person you know?
- If it sounds too good to be true, it probably is. It's most unlikely that someone will want to give you money, or give you access to a secret part of the Internet
- Your bank, or any other official source, should never ask you to supply personal information from an email
- Try to check any claims made in the email through some other channel. For example, by calling your bank to see if they actually sent you an email or doing a quick internet search on some of the wording used in the email

Remember – do not follow any links, or reply, until you're certain a sender is genuine.

3. Sources of further information and training

In addition to the resources mentioned above, the following may be helpful:

- Information Commissioner's Office – Data Protection and Coronavirus Information Hub https://ico.org.uk/global/data-protection-and-coronavirus-information-hub/
- HMRC examples https://www.gov.uk/government/publications/phishing-and-bogus-emails-hm-revenue-and-customs-examples
- Companies offering staff awareness training and simulated phishing attacks:
    - PurplePhish – www.purplephish.com
    - IT Governance www.itgovernance.co.uk
    - Cyber Security Awareness – www.cybersecurityawareness.co.uk