View this email in your browser

www.onewest.co.uk

One West

Important - Please pass to your Business Manager

Cyber Security Attacks - COVID-19 emails

COVID 19 EMAILS

We are seeing a spike in email cyber attacks which are using **Covid-19** as a means to lure people in to clicking links or opening attachments. Examples are:

- *Latest Covid-19 map*
- *Schools to remain closed until Xmas*
- *You’ve been added to Project X on MS Teams*
- *March Payroll Delay*
- *Covid-19 Tax Refund*
- *Virus now airborne (purporting to be from the World Health Organisation)*

Many of us are now working in different ways and no longer have a colleague sat close by to ask for advice. It is essential at this time to ensure you still employ your usual approach to emails, and not rush into clicking or replying – these attacks are designed to trick you into clicking a link and providing your login details, or opening a malicious attachment (which will run code in the background). We all need to remain vigilant.

The two main rules are:

- Was I expecting this email?
- Does it look and feel right?

To help you with the last rule - here are 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 someone 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 Google search on some of the wording used in the email.

Whilst email seems to be the most frequent channel, attackers are also using phone calls (known as **Vishing**) and text messages/SMS (known as **Smishing**) – so remain please remain vigilant on other communication channels.

For official information about coronavirus, please refer to trusted resources such as the Public Health England or NHS websites.

If you think an email is suspicious, follow these steps:

- Don’t open any attachments or click on any links
- Report the email to your IT provider

If you are unsure then:

- Hover (don’t click!) on the link - it will show you the address it’s trying to take you to
  - Beware - The address may look genuine, but have some slight spelling differences, or use of symbols/numbers to trick the brain into thinking it reads something legitimate
- Consider how you would verify the validity of it

- Can I ring the sender on a trusted line (e.g. obtained from official website, or from my contacts)?

If you have clicked a link then don’t panic – but ensure you change your password and report it to your IT provider ASAP.

Thanks

The One West team.

Our mailing address is:
One_West@bathnes.gov.uk

Want to change how you receive these emails?
Drop us a line - we will be happy to help