One West

Please pass to your Business Manager

Prevention of Cyber Attack via emails

How to spot & deal with illicit emails

Many of us now work in different ways and no longer have a colleague sat close by to ask for advice.

It is essential to have a safe approach to emails, and not rush into clicking or replying.

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:

#1 Was I expecting this email?

#2 Does it look and feel right?

To help you with the last rule - there are some ways to spot phishing emails

- Many phishing emails have poor grammar, punctuation and spelling. Watch out!

- Is the design and overall quality what you'd expect from the organisation the email is supposed to come from – if not be careful.

- 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 or 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. Watch out if it happens!

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 hover (don't click!) on the link - it will show you the address it's trying to take you to. Does it look legitimate?

- Consider how you would verify the validity of it – for instance can you ring the sender on a trusted line?

Finally - if you have clicked a link then don't panic – but ensure you change your password and report it to your IT provider ASAP.

One West is working with over **450** organisations throughout the South of England offering Specialist Professional Services. You can check us out via www.One_West.co.uk
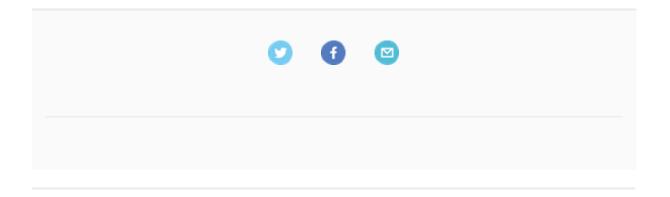
If interested & you want to talk to us about any of our services you can ring on 01225 395959 or contact, Steve_Debruin@bathnes.gov.uk .

We can offer a range of support including team training to help in what can be a tricky area.

You can also see what we do via www.onewest.co.uk

It would be great to hear from you.

The One West team