PROTECTING REMOTE WORKERS AND YOUR BUSINESS

How to detect suspicious emails

Spam and phishing attacks are becoming more complex to detect and more difficult, as a user, to identify. We've put together some guidance to help you identify malicious emails you and your team might receive.

Phishing Attacks are more common than ever. This is a type of fraud in which a hacker will attempt to gather personal information or credentials by pretending to be from a reputable source or brand.

What should you and your team do?

- Be extra vigilant with any email sent to you by a sender you don't recognise.
- Be wary of opening any attachments, even those from trusted sources, if you weren't expecting an attachment or the attachment is of a different type than would normally be sent.
- Verify the email address that the email has come from. If the display name, i.e. Bill Gates, and the email address, i.e. totallygenuine@outlook.com, don't match, treat it as suspicious.
- Look, but don't click. Instead, hover your mouse over the link to confirm the address shown is where the link will take you, such as www.google.co.uk
- Check for spelling mistakes. Legitimate emails very rarely contain spelling mistakes or poor grammar.
- Look at the greeting. Vague address information such as "Dear valued customer" could be from a suspicious source.
- Never give out personal information. Legitimate emails from banks and other companies will not ask for personal credentials such as passwords.

- Be wary of urgent or threatening language in the subject line. Using urgency and fear is a common tactic to trick you into submitting information. Common terms are "Your account has been suspended" or "Unauthorised login attempt."
- Review the signature. A lack of detail on how to contact the sender suggests a phishing attempt.
- Don't believe everything you see. Just because an email has convincing branding, logos, language and a seemingly valid email address, does not mean it is legitimate. Be sceptical with your email and if in doubt please contact whoever looks after your IT for a second opinion.

Be aware of social engineering

Covid-19 has caused a surge in attackers exploiting users working from home using social media platforms and phishing emails.
Users need to be specifically aware of the following:

Phishing emails, vishing and/or SMS

- If you receive an email or SMS asking for personal information, **check the sender** to ensure it's from someone you trust and know.
- Vishing involves you receiving a call and attempting to deceive you into handing over personal information. **DO NOT** provide any personal identifiable information.

One thing you can do straight away

Microsoft has introduced a new feature called **Office 365 Advanced Protection**. This consists of Safe Attachment, which checks email attachments, and Safe Links, which checks links in emails.

This is a quick configuration (done remotely) for anyone using the Microsoft 365 Business Plan. If you have other Microsoft 365 plans, a bolt-on is available.

To get started with Office 365 Advanced Protection, call us on 0330 333 6400 or email us at info@mpsplc.co.uk