Cyber Security
Protecting Your Information

Why you should use Multi-Factor Authentication (MFA)

MFA adds an extra layer of security to your accounts and minimises the risk of someone accessing your account by obtaining or cracking your credentials. MFA means that alongside your password, a potential intruder also needs to have access to your authenticator app (usually on your mobile phone) to be able to access your systems. It is important to never approve an authentication request unless you are personally signing into the associated account at that time.

How to spot a potential threat

Whilst MFA is an effective way of ensuring that the only person able to access your information is yourself, it isn't completely foolproof. Being aware of how to spot a potential concern, especially in relation to your email account, is crucial to safeguard your credentials.

Steps you can take:

- **Check the sender** – Even if the display name shows as someone you know, always check the sender's email address to see if it's legitimate or not.
- **Suspicious links** – If an email contains a link, always hover over the link first to see where it leads, if the URL looks suspicious then do not click it.
- **Unexpected emails or email attachments (especially invoices)** – If an email is unexpected or contains an attachment that you weren't expecting (often an invoice attachment or link), do not open these until you have spoken to the sender directly.
- **Urgent language** – Spam emails may use urgent language to pressure you into action quickly.

Information provided by Roberts & Morrow Technology (RMT)