Phishing attacks:
Defending your organisation

National Cyber Security Centre
a part of GCHQ

A multi-layered approach - such as the one summarised below - can improve your resilience against phishing whilst minimising disruption to user productivity. This approach provides multiple opportunities to detect a phishing attack and stop it before it causes major harm. The mitigations included are also useful against other types of cyber attack.

LAYER 1
Make it difficult for attackers to reach users.

- Implement anti-spoofing controls to stop your email addresses being a resource for attackers.
- Consider what information is available to attackers on your website and social media and help your users do the same
- Filter or block incoming phishing emails.

LAYER 2
Help users identify and report suspected phishing emails.

- Relevant training can help users spot phishing emails, but no amount of training can help them spot every email.
- Help users to recognise fraudulent requests by reviewing processes that could be mimicked and exploited.
- Create an environment that lets users seek help through a clear reporting method, useful feedback and a no-blame culture.

LAYER 3
Protect your organisation from the effects of undetected phishing emails.

- Protect your accounts: make authentication more resistant to phishing (such as setting up MFA) and ensure authorisation only gives privileges to people who need them.
- Protect users from malicious websites by using a proxy services and an up-to-date browser.
- Protect your devices from malware.

LAYER 4
Respond to incidents quickly.

- Define and rehearse an incident response plan for different types of incidents, including legal and regulatory responsibilities.
- Detect incidents quickly by encouraging users to report any suspicious activity.