AWARE | SECURE | RESILIENT

5 STEPS TO CYBER-SECURITY:

3 AVOID PHISHING ATTACKS

Implement the right measures to reduce the chances of your business being the victim of phishing attacks or any other cyber-security issues.

What is phishing?

Untargeted, mass emails sent to many people asking for sensitive information (such as bank details) or encouraging them to visit a fake website.

What is spear phishing?

Phisher is deliberately attacking a specific person and has crafted an email containing personal information to make them click.

WORK ON YOUR SECURITY CULTURE

Creating an accepting and transparent culture will provide a foundation to address phishing, and any other security matters, with employees. Your campaign will have a much better impact with an actively engaged workforce.

- ✓ Readily available training resources and materials.
- ✓ Awareness posters, occasional reminder emails or as part of newsletters.

TECHNICAL DEFENCES

Invest in appropriate technical and network controls to limit the amount of potentially malicious emails that employees may receive. The less malicious content accessible to employees, the lower the chance of them falling for a scam, meaning limiting exposure.

- ✓ Use reputable mail and web gateway protection products in addition to your anti-virus software.

ESTABLISH TRAINING AND CONSIDER SIMULATIONS

Provide regular training for your employees so that they are reminded to remain vigilant and know what to do when they receive a phishing email. You may wish to consider implementing phishing simulations for a more hands-on training experience.

- ✓ Routine security training and refresher courses.
- ✓ Consider different delivery styles to find most beneficial and effective for employees.

ENCOURAGE REPORTING

Some phishing attempts, especially spear-phishing attempts, can be difficult to spot. It is important that you encourage a supportive environment for employees to come forward if they feel they may have responded to something that they now regard as suspicious.

- ✓ Accessible and easy to understand reporting procedures.

ENCOURAGE DIGITAL FOOTPRINT MANAGEMENT

Spear phishers often harvest details of employees from their online profiles and use them to make their approaches more convincing and persuasive. Employees should be encouraged to consider what information about them is available online and look to reduce their digital footprint wherever they can.

Top tips for managing your digital footprint:

1. Search online to see what people can find out about you. Remember, it might not just be you creating your digital footprint. Make sure you know who else is posting about you online as well.
2. Review what personal and work-related data is available online about you. Can you delete parts or ask them to be removed? Think carefully about what you share – you don't always know who's looking at it, how it will be protected, or who it might be shared with.
3. Regularly monitor your digital footprint – Social media privacy settings can change, the devices you use can change, and the information about you can change as you and others add to it.

USEFUL RESOURCES

OCSIA Knowledge Base: www.gov.im/ocsia

UK NCSC Information for Small & Medium Sized Organisations: www.ncsc.gov.uk/section/information-for/small-medium-sized-organisations

UK NCSC Staff Cyber Security Training: https://www.ncsc.gov.uk/blog-post/ncsc-cyber-security-training-for-staff-now-available