Training Aid

Email Phishing Checklist

There are no fool-proof methods to prevent phishing. But you can reduce the risk by installing anti-phishing tools and making your employees aware of the risks.

Workplace malware protection tools may not always succeed. That's why it is important to try and avoid the risks by following a few simple guidelines.

1. Keep your software up-to-date!

Ensure that you keep the software updated and mitigate the consequences of any mistake you might make

2. Be sceptical about links in branded emails

If you receive an email from a recognised brand, be sceptical if it asks you to click a link, provide your personal information or passwords.

3. Avoid oversharing personal information on social media

Avoid sharing your position, job title, location, company and even age on social media

4. Train yourself to recognise personal styles

Make yourself familiar with how colleagues and suppliers communicate with you.

5. Notify your IT team of suspicious emails

If you are suspicious of an email, then forward it to your IT team.

6. Be wary of requests from generic addresses

If you receive an email from a generic address, e.g., customerservice@, help@, hr@ itsupport@, or payroll@, always be suspicious

7. Know the red flags

Be wary of generic greetings, unusual sender information, poor formatting, spelling/grammar mistakes, dire warnings, incorrect facts, financial rewards or penalties and a lack of legally required links to subscribe.

8. Finally, trust your instincts

If it sounds too good to be true, it usually is. If it sounds too bad, it also usually is. Cybercriminals are experts at making up extreme scenarios.