Seven tips to help you recognise phishing

Tips to help you spot a phishing message and reduce the risk of cyber attacks

An email or electronic message can contain official logos or other signs of a reputable organisation, but may still come from phishers. In this article we share seven hints that can help you spot a phishing message to help reduce the risk to you and your employees.

1. Generic or informal greetings:

If a message lacks personalisation (e.g. "Dear Customer") then there is probably something amiss. Familiarise yourself with how colleagues, suppliers, customers and companies communicate with you. If it doesn't feel right, then it probably isn't.

2. A request for personal information:

Frequently used by phishers, usually avoided by banks, financial institutions and most online services, illicit communications will ask for personal details or try to trick you into sending money or steal your details to sell on.

3. Poor language:

If you notice unfamiliar grammar, a strange tone of voice or broken English, then beware. However, just because there are no spelling mistakes does not mean it's safe - you need to look out for the other signs too.

4. Unexpected correspondence:

Unsolicited contact from a bank or online service provider is highly unusual and thus suspicious. If you receive something that you are not expecting then exercise extra caution.

5. A sense of urgency:

Are you being asked to act urgently? Within 24 hours? Common phrases include 'send these details within 24 hours' or 'you have been a victim of crime, click here immediately'. Phishing messages often try to induce rapid and less-considered action to create fear and uncertainty.

6. An offer you cannot refuse?

If the message sounds too good to be true, it almost certainly is. Don't be fooled into thinking that someone wants to give you money, to amazingly improve your life, or give you access to a magic, secret part of the internet.

7. Suspicious domain:

If you are suspicious, then check the sender's domain name. Scammers have become very adept at representing an official domain name but there are usually clues that all is not well.

If in doubt, then the best course of action is to check with your IT team or support provider. Report your concerns as it's always better to be safe than sorry.