6 Ways to protect yourself from "phishing".

Phishing - a message or email that contains "bait", with the intention of getting you to "bite".

The origins of phishing go back to the days of "Nigerian Prince" emails, where you may have received an email purportedly from a wealthy foreigner asking for help in retrieving their money by getting it out of the country. These emails were rarely targeted and were spammed out in huge quantities.

The problem for the cyber criminals running these campaigns is that they were not targeted and were often full of grammatical errors - most people receiving them realised they were a scam.

Today, many phishing messages being sent are more carefully crafted and often targeted, making it much harder to tell, at a glance, whether they are genuine or a scam.

Phishers rely on information obtained elsewhere to design their campaign and target you, so attempting to limit the information out there will help protect you.

1: Limit publicly viewable information. Don't, for example, put information useful to scammers on social media. Keep your profile private if possible - this always applies to social media but for business sites like LinkedIn, where you may wish the profile to be public, limit the amount of data visible to those you are not connected with.

2: Don't share sensitive data with web sites or organisations if it can be avoided. This includes things like your date of birth with shopping sites, names of your children or pets, or even your bank sort code. Consider lying when answering security questions (but keep a note of the answers) - i.e. use alternatives.

3: As with point 2, do not complete random surveys, questionnaires, polls or quizzes that seek to extract information (even your email address). That information can be used for follow-up attacks, to make a scam seem more believable.

4: Learn how to spot scam and phishing messages. A "first glance" check on a message is no longer enough. Scammers duplicate wording and logos from legitimate correspondence to make their copy. Tell-tale signs include messages with a sense of urgency, fear or panic. Always pause. Wait a few moments. Call the organisation in question on an existing number or where you've looked up the number. Never call the phone number listed in the message - it's likely to be the scammers. Links in emails are often fake and usually disguised. The text on the screen may not be the actual link. Always hover over a link (on a PC) or "long press" (on a phone) to reveal the true link if you're unsure. Remember that cybercriminals will often register "similar" domains to genuine ones. e.g. royal.mail.tracking-my-parcel.com.

5: Ensure you use robust, commercially obtained cybersecurity software. Also known as "anti-virus" software, today these security suites for your PC or Mac are much more than just anti-virus packages and will help protect you if you fall for a scam message.

6: Consider upgrading your email solution by adding an email filtering service. These services pre-filter email before it hits your inbox, trapping 99% of phishing, malware, scam and spam emails. They do this using artificial intelligence and will greatly reduce your exposure and risk. They are much more effective than the default protection offered by your mail provider (e.g. Microsoft 365) and better than just anti-spam filtering.