Six ways to spot a phishing attack

What is phishing and how can you spot it?

Phishing is an attempt, usually through email, to gather personal information or to compromise technology for the purpose of financial gain or malicious activities. Phishing emails typically include a link to a fraudulent site or an attachment containing malware. You should also be aware of QRishing – phishing that tricks you into scanning a QR code that sends you to a malicious web page. Every day millions of phishing emails are sent out to unsuspecting victims all over the world. Cybercriminals often launch topical attacks to get attention, using data breaches or national and international events to their advantage. Some are easy to detect as fraudulent but others can be much more convincing. Cybercriminals are also utilising capabilities within Generative Artificial Intelligence to create convincing phishing emails which are harder to spot.

How can you tell a real email from a scam one? It can be tricky, there is no magic bullet for detecting them but be alert to the fact that, one day, you will receive a phishing email. Most successful scams use emotions to get reactions so when you receive something which is unexpected, makes you feel something or asks you to take action – slow down and think carefully. Reading through and remembering our 'Six ways to help spot a phishing attack' is a strong start.

Adviser Solutions

Fidelity INTERNATIONAL

1 The message has a suspicious or mismatched URL

If you are suspicious, always check the integrity of any embedded URLs. Phishing message URLs may seem to be perfectly valid but if you hover your mouse over them you can reveal the real destination address. Check the details carefully as some addresses can seem to be genuine but have subtle differences (i.e. www.amazon.com vs. www.amazon.org). On a mobile device you can perform the same function by holding your finger on a link for a couple of seconds.

2 It has poor spelling or grammar

When a major organisation sends out a message it's usually checked for spelling, grammar, and legality. If a message is filled with spelling mistakes it probably didn't come through a major corporation's publicity or legal department. Remember, not all phishing emails will include these kinds of mistakes and they are appearing less frequently with advances in generative artificial intelligence. Remember it's important to concentrate on what you are being asked to do, not just how you are being addressed.

3 It asks for personal information, such as passwords

No reputable company will ever ask you to send or confirm passwords or log-on details via email, or get you to click on a link that takes you to a website where you can login. If you're in doubt whether the email is genuine, find the official company website or telephone number independently and contact them yourself to check.

4 You're not expecting anything from the sender

You've won a big prize or competition! But did you, in fact, enter one? A financial company is 'replying' with the spreadsheet you requested, but did you ask them for anything in the first place. Chances are this is a phishing email. Be especially wary of unexpected emails with attachments, these can be harmful and could infect your computer with malware.

5 You must act now!

Messages that say you must 'Reply Now' to avoid losing money, having your access cut-off or account deleted, are usually trying to get you to act without thinking. Take your time and investigate. Don't feel rushed into doing something you shouldn't. Remember, phishing emails are often designed with this kind of 'panic response' built in so if you feel panicked or rushed, take a moment.

6 Something just seems wrong

It would be fantastic if we could cover every way a phishing attack could happen here but the truth is the best defence you have against fraud is your common sense. Sometimes things just don't seem quite right, learn to trust that feeling. A phishing attack is a form of social engineering, they are playing with your mind, so stay alert and be ready.

If you think you've identified a phishing email, take action...report it via your local email reporting service

UKM1123/LM/QC/1124 [WF1589770]