JEFFMAYNARD.COM

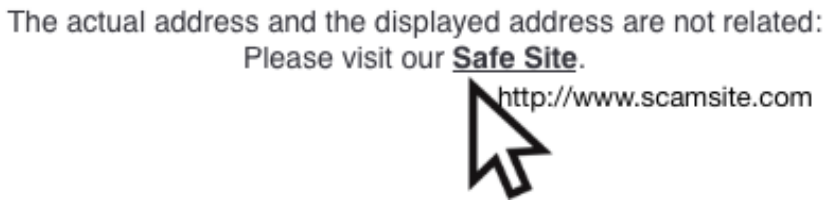
CDSV
CYBER AND DIGITAL SPECIALS AND VOLUNTEERS

PHISHING

Criminals us fake mails designed to look like those you might receive from your bank, building society, HMRC, the NHS, Amazon, Royal Mail, various courier companies and others (please note that this is not an exhaustive list - always be on your guard when receiving unexpected emails or those urging some action).

This practice, known as **phishing**, will try to persuade you to click a link, provide personal or financial information, or download an attachment. We advise that you delete such emails immediately. If you think the email might be genuine, contact the sender but using a telephone number or email address sourced by yourself (do not use any telephone number or email address in the suspect message).

A link in such a message may look genuine but hovering your mouse over it (or tapping and holding on a tablet or phone) will popup the real address the link is going to take you to:



Never give any password, PIN, financial information etc in response to an email request.

For more Police advice on Phishing tap **here**.

Social media platforms, such as FaceBook, Instagram and others, are also used to entice potential victims to part with information of value to criminals. Apply the same safeguarding checks to messages received *via* social media and protect all your accounts with strong passwords (and 2FA if available) - see the related paper.

Criminals also use **text messages** to try to persuade you to follow a link where they will ask for personal and financial information. No legitimate organisation (bank, government, police or commercial company) will use text messaging to seek personal information. The use of text (SMS) messaging is known as **smishing**. Examples: