Crime prevention advice for

Phishing Emails

I've received a suspicious email

Our guide to spotting and dealing with phishing emails.

If you haven't clicked any links in the email, that's good. Until you're certain that the sender is genuine, you should not follow any links, or reply.

The next thing to do is try and identify whether the email is a scam, or genuine.

Here's some tips on spotting phishing emails

- Many phishing emails have poor grammar, punctuation and spelling.
- Is the design and overall quality what would you'd expect from the organisation the email is supposed to come from?
- Is it addressed to you by name, or does it refer to 'valued customer', or 'friend', or 'colleague'? This can be a sign that the sender does not actually know you, and that it is part of a phishing scam.
- Does the email contain a veiled threat that asks you to act urgently? Be suspicious of words like 'send these details within 24 hours' or 'you have been a victim of crime, click here immediately'.
- Look at the sender's name. Does it sound legitimate, or is it trying to mimic someone/an organisation you know?
- If it sounds too good to be true, it probably is. It's most unlikely that someone will want to give you money, or give you access to a secret part of the Internet.
- Your bank, or any other official source, should never ask you to supply personal information from an email.

Try to check any claims made in the email through some other channel. For example, by calling your bank to see if they actually sent you an email or doing a quick Google search on some of the wording used in the email. NOT THE NUMBER THEY GIVE YOU!!!

Warwickshire County Council

Warwickshire POLICE

Philip Seccombe Police and Crime Commissioner for Warwickshire

Phishing Emails

Followed the advice?

The above advice will go a long way to helping you secure yourself online but if you do spot a suspicious email, flag it as Spam/Junk or Suspicious in your email inbox. This will take it out of your inbox, and also tell your email provider you've identified it as potentially unsafe. You can report suspicious emails, phone calls or SMS messages to Action Fraud (actionfraud.police.uk).

For further information, we also have the following guidance pages:

- Passwords
- Malware and Ransomware
- Recover an Infected Device
- Back Up Data
- Antivirus
- Two-Factor Authentication