Phishing – Advice on how to avoid getting caught

What is Phishing?

Phishing is an attempt used by criminals and fraudsters to obtain your personal information and typically happens when you're sent a convincing looking but fraudulent email, although you may be contacted by phone.

If you've got an email address the odds are you've already been phished. Ever received an email about a parcel delivery you never ordered, or asking you to revalidate your account credentials? These are typical phishes which are relatively easy to spot, but the criminals behind them are smart and keep coming up with more plausible scenarios

These emails are often sent to thousands of individuals in the hope that some will be hoodwinked into supplying personal information. This may include user names, email addresses, passwords, bank account, and credit card details.

These phishing attacks will typically encourage victims to enter details on a fake website which often seems to come from a legitimate organisation.

Look out for phishing emails that contain:

•Casual or informal wording that's not in the normal style of an email from a legitimate company.

•Familiar language or tone but poor grammar and spelling.

•'Verify your account' request - banks will never ask you to enter full account details, passwords or PINs onto a website.

•'There is a secure message waiting for you' - these messages work by putting the emphasis on reading a message - not your actual account. However, the link in the email will still ask for your personal account details.

•'If you don't respond within 48 hours, your account will be closed' - such messages convey a sense of urgency that can make you respond immediately without thinking. Phishing emails might even claim that your response is required because your account may have been compromised.

•'Click the link below to gain access to your account' - sophisticated email messages can contain links or forms that you may fill out just as you would do on a legitimate website.

•'Dear Valued Customer' - phishing emails are usually sent out in bulk and often do not contain your first name or surname

BT
Cumbria County Council
Department for Culture Media & Sport
Funded by UK Government
NOW'S THE TIME FOR SUPERFAST BROADBAND
gov.uk/gosuperfast
HM Government

You will get phished - so how do you spot the bait, and what should you do?

Proceed with caution!

Emails can come from anywhere, so until you are totally sure an email is genuine…

- DON'T click links or open attachments; these may infect your computer with a virus.
- DON'T reply to the email, or unsubscribe from the emails.
- DON'T ring any phone numbers in the email.

Remember - company logos can easily be forged in an email, making it look more realistic.

Is it a bait? There are some clues you can look out for…

- Is your name missing? Genuine emails from reputable companies personalise their emails with your name
- Are you asked to do something like validate account credentials or re-activate an account?
- Is it requesting personal data or bank details?
- Did the email come out of the blue? Companies don't just contact you asking questions or offering things without you doing something first.
- Has the email been sent to multiple recipients?
- Is it something related to a current news event? Often criminals will use security incidents that have hit the news to plan attacks e.g. a company lost its customers passwords and they need to be reset.
- If it's from someone you know, does it look and sound right?
- Is the grammar right, are there spelling mistakes?

Check for hooks

- Does the sender's address match the organisation that supposedly sent the email?
- Hover over all links to show where they really go
- Contact the sender organisation. But NEVER trust any contact details or links in the email; always use details from the organisation's website

Get away

- Deleting the message is the safest option
- Don't click links saying unsubscribe, this just shows the criminals they've found an active email account

Finally: further protection

- Anti-virus and software updating

  Make sure your devices have the latest anti-virus definitions, up-to-date software and patches. This may still protect you if you are a phish victim. Security loop-holes are regularly discovered in software, and lots of scams exploit these vulnerabilities. To run a selfcheck on your computer, **go to the anti-virus software** and run a scan.

Admin-rights

Some malicious software needs administrator privileges to install on your computer. Avoid running your PC with administrator access except when really necessary.