

phishing

ISSUE 57

SCAMS AWARENESS NEWSLETTER

AUGUST 2025

WELCOME TO OUR

Monthly Newsletter

Phishing Scams



In this newsletter:

- Phishing scams and how to recognise a phishing scam - P2
- Warning signs, top tips and example of a phishing scam - P3
- Reporting a scam, top tips and IT support/classes - P4

Phishing scams are fraudulent messages—usually emails or texts—that pretend to be from trusted organisations, like banks, utility companies, the police or government services, to trick you into sharing personal information such as passwords, bank details, or credit card numbers.

Recently, Age UK National, was the victim of a phishing campaign. Fraudulent emails targeted individuals outside our organisation, including local Age UK Partners and even family members of colleagues. The fraudsters sent out fake emails claiming to offer a "Free Age UK Health Monitoring Kit." Emails like these are designed to misuse Age UK's trusted name and trick recipients into clicking on links that lead to malicious websites.

This scam, known as a phishing attack, is designed to look like it's coming from a trusted organisation. In reality, the goal is to get you to click on dangerous links or provide personal information like bank details, passwords, or credit card numbers.

Phishing Scams

Unfortunately, scams like this are becoming more common and more convincing. That's why it's important to stay informed and cautious. These scams are designed to look real but can lead to dangerous websites, steal your identity, or install harmful software on your device.

Below, we've shared a few simple ways to spot a suspicious email and protect yourself.

How to Recognise a Phishing Scam:

Scammers are deceitful and use underhand tactics to keep up with current news or trends. They often create convincing stories to catch your attention and push you to act quickly—like clicking a link or opening an attachment.

They may pretend to be from banks, credit card companies, utility companies or even government agencies and may:

- Claim they've noticed suspicious activity on your account
- Say there's a problem with your payment details
- Ask you to "verify" or "confirm" personal or financial information
- Send a fake invoice or receipt you don't recognise
- Tell you that you're due a refund from the government
- Offer discounts, freebies, or fake coupons
- Ask you to click on a link that installs harmful software
- Offer free upgrades of your service package

Even if the email looks official or comes from a known sender, pause and think before you click. Scammers can fake email addresses and company logos to look very convincing.



Warning signs to watch out for:



Here are some common red flags that could indicate a phishing attempt:

Generic greetings

- Messages that say “Dear Customer” instead of using your name.

Urgent or threatening language

- Phrases like “Act now!” or “Your account will be suspended!”

Suspicious links or attachments

- Never click unless you're sure the message is genuine. Hovering over links doesn't always help—some scammers can disguise links to look legitimate.

Unfamiliar or misspelled email addresses

- Look closely—just one wrong letter or number can signal a scam.

Spelling and grammar mistakes

- While many phishing emails have poor spelling, not all do. Don't rely on this alone.

Tips to stay safe:



Be cautious of any unexpected messages—even if they seem to come from a trusted source.

Never give out personal information in response to an email or text.

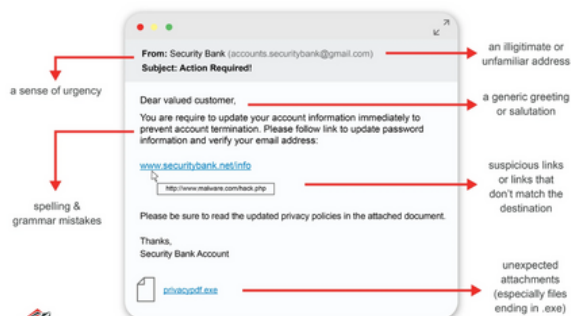
Don't update payment details through links in emails/texts. Reputable companies will never ask for that.

Verify messages by contacting the sender directly using a phone number or website you trust.

If you're ever unsure, talk to someone you trust.

Examples of a phishing scam:

WATCH OUT FOR...



What to do if you clicked a link in a phishing email:

Don't enter any information: If the link took you to a page that asked for your personal or banking details and you haven't entered anything—you're likely still safe. Just close the website immediately.

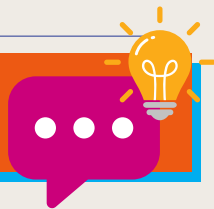
Disconnect from the Internet (optional, if possible): If you're worried your device may have been infected, you can temporarily disconnect it from Wi-Fi or unplug it from the internet.

Run a security scan: Open your antivirus software and run a full scan of your computer, tablet, or phone. Most devices have built-in security tools, or you may have antivirus software installed already. If you're unsure how to do this, ask a trusted friend or family member to help.

Change your passwords: If you entered any passwords (email, banking, shopping accounts), change those passwords immediately, especially for your email account. Your email is often the key to everything else.



Top Tips:



- ✓ Use strong passwords that are hard to guess. National Cyber Security Centre: Three random words. If remembering them is difficult, consider writing them down and storing them somewhere safe, like a locked drawer.
- ✓ Contact your bank (if you provided any banking details): If you entered any financial information, call your bank on 159 right away. They can help protect your account.
- ✓ Watch for unusual activity: Keep an eye on your bank statements, email, and online accounts for anything unusual—such as unfamiliar purchases, login alerts, or password reset messages.

Reporting a Scam



If you receive a suspicious email:

- Don't click on anything or reply
- Forward it to report@phishing.gov.uk
- Delete it from your inbox and your trash folder



IT support/classes:

Contact your local library and make an appointment with an IT buddy for digital support.

[AbilityNet](#) is a charity helping older people and people with disabilities with free technology support. 0300 180 028

[Digital Cheshire](#) hold regular drop-ins and free courses. digitalcheshire@cheshireeast.gov.uk

[Disability Information Bureau](#) offers free IT courses (group sessions and 1:1's). 01625 501 759

[Springboard](#) offer digital skills courses. 01260 290 682

If you are affected by the content of this bulletin, you can talk to us. Our Scams Awareness and Aftercare Team can offer free support, advice and guidance. Contact our team today on:



01625 612958 (OPTION 5)



scams@ageukcheshire.org.uk