A quarter of UK email users receive suspicious emails every day

Ofcom research has found that email is one of the most common channels for scams in the UK.

Classic signs of a scam

While scammers are becoming increasingly savvy, some reliable signs that a message or call you received or something you came across online could be a scam are:

- Being contacted unexpectedly.
- Messages containing links.
- Being asked to share personal or financial information.
- Being asked to make an urgent payment.
- Being asked not to share any details with friends or family.
- Buying from a retailer with missing or vague contact details.
- Products or investments that are too good to be true.
- Poor spelling and grammar.

  Be cautious of unfamiliar greetings, unsolicited messages, grammar errors, and a sense of urgency.

  Watch out for suspicious links or attachments, requests for personal information, and inconsistencies in email addresses

- **Do not respond to unsolicited emails**:
  - Avoid replying to suspicious messages. Responding confirms your active email address to scammers.
- **Report suspicious messages**:
  - Report scam emails to your email provider promptly.
- **Avoid sharing personal information**:
  - Never provide sensitive data via email unless you are certain it's legitimate.

. Can You Get Scammed by Replying to a Text?

The truth is that, *yes*, it's possible to get scammed by replying to a text message.

Fraudsters send billions of fake text messages every month hoping that a small percentage of people will respond. And their scams are getting harder and harder to spot. Today, scammers impersonate delivery services, government agencies like the IRS and DMV, financial institutions, or even family members via text.

What to do if you clicked on a link in a spam text message:

- **Disconnect from your Wi-Fi and/or mobile network.** Hackers need an internet connection to access your device. Shutting down your service can block them from accessing your device and sensitive data.
- **Scan your device for malware and viruses.** Once you are offline, use antivirus software to scan your device for malware and remove any malicious code.
- **Change your passwords and enable two-factor authentication (2FA).** If scammers get access to your phone, they can hack into your accounts. Update all of your passwords as soon as possible and enable 2FA on any account that will allow it.
- **Update your device and apps.** Many updates include security patches that help protect against new cyberthreats.

1. **Use strong passwords**:
    - Regularly update your passwords and avoid using easily guessable ones.
2. **Keep your operating system up to date**:
    - Install security patches promptly to stay protected.
3. **Stay informed**:

How to report scams

Ofcom's research also found that one of the most common reasons for not reporting a scam was that people didn't know where to report it to.

Reporting scams is important as it's the most effective way to get a scam taken out of circulation.

Depending on the type of scam you've received, there are different ways to report it:

- **Text messages:** forward it to 7726. You can report scam WhatsApp messages by pressing and holding the message before selecting ‘report’.
- **Emails:** forward scam emails to report@phishing.gov.uk. You can also select ‘report spam’ on Gmail, ‘report phishing’ on Hotmail or send scam emails to abuse@yahoo.com if you’re using a Yahoo account.
- **Calls**: you can report scam calls received on your mobile to 7726. On WhatsApp, open the WhatsApp chat with the dodgy phone number and tap 'block.' You can report the contact by tapping 'report contact'.
- **Websites:** suspicious websites should be reported to the National Cyber Security Centre (NCSC)

- **Social media:** to report a scam group, page, or profile on Facebook, select the three dots on the right-hand side of the page and click ‘report’. On Instagram, you can press the three dots in the top right corner of a post or profile and select ‘report’. On X, formally known as Twitter, select the three dots and then ‘report.’