

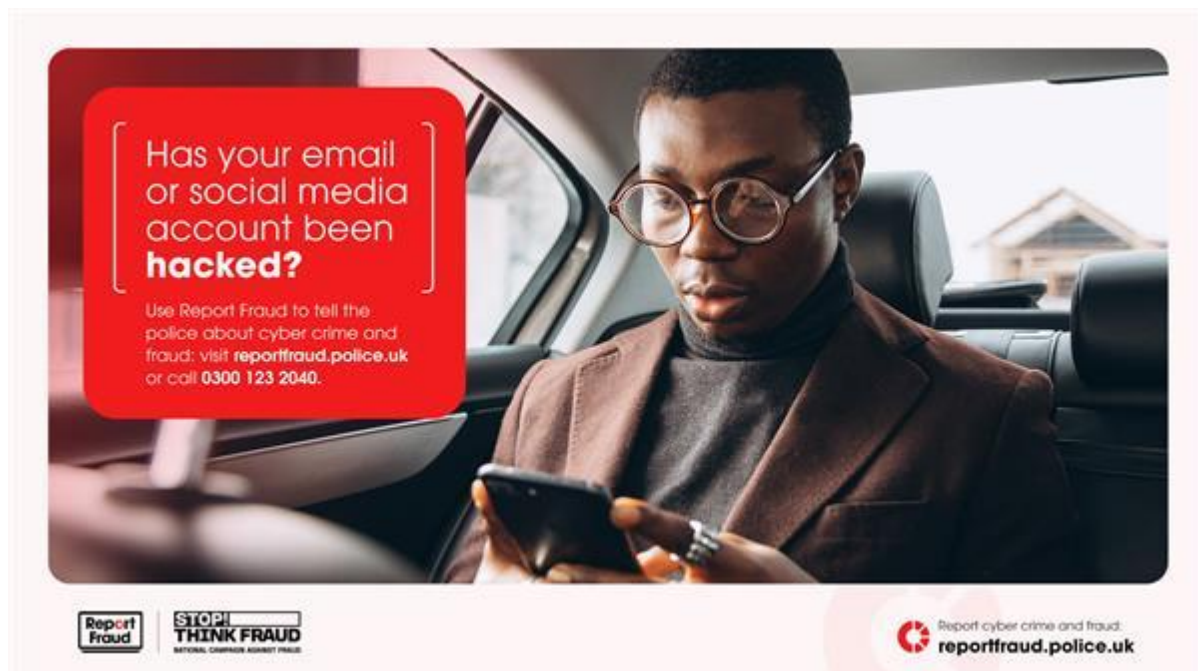
ALERTS

TRADING STANDARDS

15/10/2026

Switch to Passkeys: Protect Your Accounts as Email and Social Media Hacking Soars

Report Fraud is urging the public to protect their online accounts after stolen sums from email and social media hacking surged by 417 per cent in the last year. Reported losses rose from £1.2 million in 2024/25 to £6.3 million in 2025/26, while reports of account hacking increased by 34 per cent, making it the most reported form of cyber crime in the UK.



Other types of account takeovers were also identified within reports, including gaming and streaming accounts, as well as travel and online delivery accounts. As part of Cybersecurity Awareness Month, Report Fraud has launched a campaign encouraging people to better protect themselves online by switching to passkeys and strengthening account security.

Account hacking occurs when criminals gain unauthorised access to an email, social media or online account and use it to commit further fraud. Once an account has been compromised, fraudsters may impersonate the account owner to target family and friends, request money, sell

fake tickets or carry out other scams. One of the most common themes identified from reports is criminals using hacked accounts to impersonate trusted contacts.

What starts as a single compromised account can quickly have a wider impact. Victims may lose access to important accounts, have personal information exposed and face the distress of knowing criminals could be using their identity to target others. Friends, family members and colleagues may also become victims if they mistakenly trust messages sent from a hacked account.

The good news is that there are simple steps everyone can take to improve their online security and make it harder for criminals to gain access.

Protect yourself online

- Use passkeys wherever they are available. Passkeys are more secure and easier to use than traditional passwords. Where passkeys are unavailable, use strong, unique passwords generated by a password manager and enable two-step verification whenever possible.
- Review your privacy settings. Make sure your social media content is only visible to the people you want to see it, such as friends and family.
- Be careful about sharing personal information online. Details such as your birthday, where you live, family relationships or pet names can be used by fraudsters to build a picture of you and make scams more convincing.
- Verify unexpected messages. If someone you know contacts you through social media or email, don't automatically assume it is really them. Contact them through another method, such as a phone call, text message or in person, before responding.

If you believe your account has already been hacked, report it to Report Fraud and seek advice on recovering access and securing your accounts.

Join the Report Fraud Social Media and Email Hacking Webinar

As part of Cybersecurity Awareness Month, Report Fraud is hosting a webinar on protecting your email and social media accounts from hackers and fraudsters. The session will cover the latest threats, practical security measures, and the simple steps you can take to keep your accounts safe from compromise. Whether you're looking to strengthen your own online security or help protect friends and family, this webinar will provide expert guidance and actionable advice.

Register your place here: <https://events.teams.microsoft.com/event/53994f64-090f-4887-8744-3422da79ad56@9386af3d-781b-4bad-8559-7170be76bad9>

WHERE TO REPORT

Protect others by reporting incidents like this.

Report suspicious texts you have received but not acted upon, by forwarding the original message to 7726, which spells SPAM on your keypad.

Report suspicious emails you have received but not acted upon, by forwarding the original message to report@phishing.gov.uk

If you, or anyone you know, have been affected by this fraud or any other scam, report it to Report Fraud by calling 0300 123 2040 or visiting www.reportfraud.police.uk

tradingstandards@royalgreenwich.gov.uk