Kent Fraud Alert System

Protect your online accounts from hackers and enable 2 step Verification

Action Fraud have issued a new warning about social media and email account hacking as new data is revealed.

This year Action Fraud and Meta are encouraging the public to protect their social media and email accounts as data shows there was a rise of social media and email account hacking reported in 2024, with a total of 35,434 reports made to Action Fraud, compared to 22,530 reports made in 2023. Action Fraud, the national fraud and cybercrime reporting service, has launched a campaign, supported by Meta, to encourage people to take an extra step of online protection by enabling 2-Step Verification (2SV) for each online account they have. The warning comes as reporting shows nearly £1 million was lost to hackers last year.

The most common motives for social media hacking were either investment fraud, ticket fraud or theft of the targeted account, reporting insights revealed.

In the reports made to Action Fraud, there were various methods of hacking highlighted, these include:

- **On-platform chain hacking -** This is when a fraudster gains control of an account and begins to impersonate the legitimate owner. The goal is to convince people to reveal authentication codes, including one-time passcodes, which are sent to them via text. Many victims of this type of hacking believe it is a friend messaging them, however the shared code was associated with their own account and the impersonator can now use it to access their account. Usually when an account is taken over, fraudsters monetise control of the account via the promotion of various fraudulent schemes, like fake tickets or crypto investment schemes, while impersonating the original account owner.
- **Leaked passwords and phishing -** The other common method of hacking is when account details are gained via phishing scams, or the use of leaked information used from data breaches, such as leaked passwords. This becomes prevalent as people often use the same password for multiple accounts, so a leaked password from one website can leave many of their online accounts vulnerable to hacking.

What can you do to avoid being a victim?

- **2-step verification (2SV) will keep criminals out of your account – even if they know your password.** Turning on 2SV gives your most important accounts an extra level of protection, especially your email and social media accounts. It can be turned on in a matter of minutes – time well spent to keep the fraudsters out. Find out how to enable it go to Turn on 2-step verification (2SV) - Stop! Think Fraud
- **Email and social media passwords should be strong and different to all your other passwords**. A good way to make sure your passwords are 'long enough and strong enough' is to combine three random words to create a unique password which is easy to remember. Find out more at Improve your password security - Stop! Think Fraud