THAMES VALLEY POLICE

TV Alert – Hacking

Increase in social media and email account hacking prompts warning to take action to protect accounts.

Protect your online accounts from hackers and enable 2SV: Action Fraud issue 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 were more than 35,000 reports made last year.

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 for each online account they have. The warning comes as reporting shows £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.

Detective Inspector Duncan Wynn, Head of Central Fraud Unit at Thames Valley Police, said:

“Social media and email remain a big part of our lives when it comes to communication, so the risk of being hacked can be concerning.

“I urge you to take some time to follow the simple steps detailed below to secure your accounts.”

“Do you have vulnerable family members who could benefit from this advice, if so? Use this as an opportunity to share and help them if required.

"Our Fraud Protection Toolkit provides plenty more tips on how to minimise the risk of fraud and is designed to help you and your communities to become empowered against the risk of fraud.

"Finally, be on the lookout for behaviour which is out of character from friends on social media and via email, for example:

- Being asked to purchase gift cards and share the codes
- Being asked to send and receive money into your bank account
- Being asked to invest in Bitcoin or Crypto

"Fraudsters prey on creating pressure which is designed to make you act quickly but Stop! Think Fraud empowers us to collectively join together to help stop fraud in its tracks."

Adam Mercer, Deputy Director of Action Fraud, said:

"As social media and email account hacking remains the most reported cybercrime this year, this Action Fraud campaign marks a critical issue for everyone who has online accounts. That's why we're raising awareness of the ways people can protect themselves online.

"Follow *Stop! Think Fraud* advice and protect yourself online: enable 2-Step Verification on each online account you have – this will help prove your identity and stop fraudsters trying to steal or access your valuable information. Secure your social media and email accounts by ensuring each password is strong and uses three random words. Remember to never share your passwords with anyone else."

David Agranovich, Security Policy Director, Meta, said:

"Scammers are relentless and continuously evolving their tactics to try and evade detection, which is why we're constantly working on new ways to keep people safe while keeping bad actors out. Two-Factor Authentication (2FA) is one crucial example of how people can add an extra layer of security to their Meta accounts, to help reduce the risk of scammers accessing your accounts. We've also started rolling out facial recognition technology to help people get back into compromised or hacked accounts and are always working on new ways to stay ahead of scammers."

In the reports made to Action Fraud, there were various different 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 that are sent to them via text. Many victims of this type of hacking believe it's 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?

- Setting up 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.
- Email and social media passwords should be strong and different to all of your other passwords. An effective 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.

Report suspicious emails by forwarding it to: report@phishing.gov.uk

Find out how to protect yourself from fraud: https://stopthinkfraud.campaign.gov.uk

If you've lost money or provided your financial information to someone, notify your bank immediately and report it to Action Fraud at actionfraud.police.uk or by calling 0300 123 2040. In Scotland, call Police Scotland on 101.

Notes to editors

- There were 35,434 email and social media hacking reports made to Action Fraud between 1 January and 31 December 2024, with losses totalling £961.5k.