Over 22,000 E-mail and Social Media Accounts Hacked

How are accounts hacked?

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 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, while impersonating the original account owner.

Leaked passwords and phishing

The other predominant method of hacking reported is leaked information used from data breaches, such as leaked passwords, or account details gained via phishing scams. 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.

How to secure your accounts

Use a strong and different password for your email and social media accounts. Your email and social media passwords should be strong and different from all your other passwords. Combining three random words that each mean something to you is a great way to create a password that is easy to remember but hard to crack.

Turn on 2-Step Verification (2SV) for your email and social media accounts. 2-Step Verification (2SV) gives you twice the protection so even if cyber criminals have your password, they can't access your email or social media account. 2SV works by asking for more information to prove your identity. For example, getting a code sent to your phone when you sign in using a new device or change settings such as your password. You won't be asked for this every time you check your email or social media.

If you live in England, Wales and Northern Ireland and have been a victim of fraud or cybercrime, report it at www.actionfraud.police.uk or by calling 0300 123 2040. In Scotland, victims of fraud and cybercrime should report to Police Scotland on 101.

If you receive a suspicious email, you can report it by forwarding the email to: **report@phishing.gov.uk.**

Find out how to protect yourself from fraud: Gov.uk/stopthinkfraud