What to do if you have been a victim?

The realisation that you may have been a victim of fraud can be extremely unnerving. There are a number of actions you can do to help limit the impact, both financially and emotionally.

Gmail, Facebook, Twitter... it does not matter what the service is, from time to time someone will find a way in. If one of your accounts has been hacked, do not panic, use these steps to help you regain control and protect yourself against future attacks.

Being locked out of the account is an obvious indication that something has gone wrong, but the signs can be more subtle. Things to look out for include attempted logins from strange locations or at unusual times. Changes to your security settings and messages sent from your account that you do not recognise are also giveaways.

1

Update your devices
The Operating Systems and apps on the devices you use should all be updated. These updates will install the latest security fixes. If you have it installed, run scan with up-to-date antivirus software. This is not usually necessary for iPhones and Apple tablets but should be applied to Android devices.

2

Contact your email provider
If you cannot access your account, go to the account provider homepage and find a link to their help or support pages. These will detail the account recovery process. Once you have regained control, check your email filters and forwarding rules. It is a common trick for the person hacking an account to set up an email-forwarding rule that sends a copy of all your received emails to them. Information on how to do this can usually be found in your provider's help pages.

3

Change passwords
Once you have confirmed there are no unwanted email forwarding rules in place, change the passwords on all accounts that have the same password as the hacked account. Then change the passwords for all the other accounts that send password reminders/resets to the hacked account.

4

Set up 2-factor authentication
This provides an extra layer of protection against your account being hacked in the future.

5

Notify your bank or other service providers
If you believe you have been the victim of an investment scam, alerting your bank, wealth manager, accountant or other professional services firm that might be a target for a hacker is essential. They can place a temporary freeze on your accounts designed to limit access to the hackers.

6

Notify your contacts
Get in touch with your account contacts, friends or followers. Let them know that you had been hacked. This will help them to avoid being hacked themselves.

7

If you can't recover your account
You may choose to create a new one. Once you have done this, it is important to notify your contacts that you are using a new account. Make sure to update any bank, utility services or shopping websites with your new details.

8

Contact Action Fraud
If you feel that you have been affected by an online crime, you should report a cyber-incident to Action Fraud using their online fraud reporting tool at **www.actionfraud.police.uk**

Protecting yourself from investment scams

The FCA ScamSmart website offers helpful support about what you can do to spot investment fraud.

Information on pension scams can be found at www.pension-scams.com

It is important to check that the companies with which you deal are authorised by the regulator, in JM Finn's case the FCA. These can be checked at the Financial Services register.

Fraud and cyber crime can be reported via ActionFraud, the UK's national fraud and cyber crime reporting centre. They also list the different types of fraud.