Securing your online accounts

Our online accounts can contain personal and confidential information and therefore are a common target for cyber-criminals. Unfortunately once these accounts have been compromised, cyber-criminals can use them to scam or extort from your friends and family.

What to do if you think your account has been compromised?

Contact the account provider. Report that your account has been compromised. You can do this by going to the help & support pages on their website.

Change and create a strong password. Use three random words to create your password – the more characters the better e.g. **GrinningSkydivingOtter£33**. Make sure your password for your email account is always different to your other accounts as this can be used to reset your online passwords.

Force all devices and apps to log out. You can usually do this from the settings menu on the app or the account provider's website.

Turn on Two Step Verification (2SV). Two-step verification (2SV), also known as two-factor authentication (2FA) or multi-factor authentication (MFA), helps to keep cyber criminals out of your accounts, even if they know your passwords.

Notify your contacts. Let your contacts know that your account has been compromised and suggest they treat any recent messages sent from your account with suspicion.

Check your bank statements and online shopping accounts. Keep a look out for any unauthorised purchases. You can always contact your bank to notify them.

If you can't recover your account. In some cases, it may not be possible to recover your account. In such cases, you'll have to create a new account. Once you've done this, it's important to give contacts your new details. *Please note the Police are unable to assist with recovering your personal accounts*.

How to protect yourself in the future?

If you receive a suspicious or unexpected message from a friend on social media, contact them via other means to check the message is genuine.

Don't click on links in unexpected or unusual messages, even if you know who it's from.

Never type in your details after clicking on a link.

Set your social media profiles to private. Oversharing on these accounts could let an attacker guess your password or reset questions.

Always double check friend requests and don't accept them from people you don't know.

Don't give your login details to anyone. Only enter your login details on the official website or app.

Never share any codes or PIN numbers.

Save copies of your photos and back up your data.

METROPOLITAN POLICE