National Cyber Security Centre
a part of GCHQ

Recovering hacked accounts

A step-by-step guide to recovering online accounts.

Whether it's your email, a social media account, or your online bank, losing access to a digital account can be stressful. This page summarises what you can do to minimise any damage, and how you can regain access to your accounts.

How to tell if you've been hacked

Check your online accounts to see if there's been any unauthorised activity. Things to look out for include:

- being unable to log into your accounts
- changes to your security settings
- messages or notifications sent from your account that you don't recognise
- logins or attempted logins from strange locations or at unusual times
- unauthorised money transfers or purchases from your online accounts

In some cases, it may not be possible to recover your account with the online service. In such cases, you'll have to create a new account. Once you've done this, it's important you give your contacts your new details, and tell them you've abandoned the old account. Make sure to update any bank, utility or shopping websites with your new details.

© Crown Copyright 2026

1. Contact your account provider

Go to the account provider's website and search their help/support pages which will explain the account recovery process in detail. It's likely to be different for each account.

2. Check your email account

Check there are no unwanted forwarding rules in your email account. Cyber criminals may can set up rules which means they'll automatically receive copies of all emails sent to your account (which would allow them to reset your passwords).

3. Change your passwords

Change the password for any account that has been hacked, and also for any accounts that use the same password. Cyber criminals know that people use the same password for different accounts, and so will try the same 'hacked' password across multiple accounts.

4. Force all devices and apps to log out

This can usually be done from the 'Settings' menus of the app or website (or it may be part of the 'Privacy' or 'Account' options). Once you've done this, anyone attempting to use your account will be prompted to supply the new password.

5. Set up 2-step verification (2SV)

2SV (which is also known as two-factor authentication or 2FA) usually works by sending you a PIN or code, often via SMS or email, which you'll then have to enter to prove that it's really you. So even if a criminal knows your password, they won't be able to access your accounts.

6. Update your devices

Apply updates to your apps and your device's software as soon as they are available. Updates include protection from viruses. Applying these updates promptly is one of the most important (and quickest) things you can do to prevent your account from being hacked.

7. Notify your contacts

Contact your account contacts, friends or followers. Let them know that you were hacked, and suggest they treat any recent messages sent from your account with suspicion. This will help them to avoid being hacked themselves.

8. Check your bank statements and online shopping accounts

Keep a look-out for unauthorised purchases. Check your bank accounts for any unusual transactions. You can contact your bank directly for further support. Always use official websites or social media channels, or type the address directly into your browser. Don't use the links in any messages you have been sent.

9. Contact Report Fraud

If you've lost money, tell your bank and report it as a crime to Report Fraud, the UK's reporting centre for cyber crime (in Scotland, contact the police by dialing 101). You'll be helping the NCSC and law enforcement to reduce criminal activity.