Sorting out a hacked account

 Prepared by Disability Equality Scotland

What hacked means

Hacked means that a criminal has got information from your device when you have not given them permission.

When you cannot access your online account anymore it is stressful.

It could be:

- your email account
- your social media account
- your online bank

This document explains what you can do to have as little damage as possible, and how you can get back into your accounts.

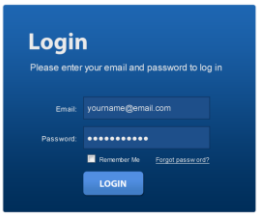
How to tell if you have been hacked

Check your online accounts to see if anything has happened that you have not agreed to.

Look for things like:

- not being able to log into your accounts
- changes to your security settings

- messages or notifications sent from your account that you do not recognise



- logins or tried logins from strange locations or at unusual times

- money transfers or things bought from your online accounts that you did not do

What to do if your account has been hacked

1. Contact your account provider

Your account provider is the company that you get your account from, for example:

- Amazon
- Barclays Bank
- Facebook

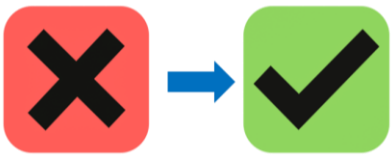
Go to the account provider's website and search their **help** or **support** pages.

These will explain the **account recovery process** – which means how to get your accounts back.

If you cannot find what you need on the website, type a question into a search engine - for example '*How to recover my Facebook account*' and then follow the link.

2. Check your email account

Check your email filters and forwarding rules.



Online criminals often set up a forwarding change so they get copies of all emails sent to your account.

This would let them change your passwords.

Get instructions about how to do the right checks on the email provider's website.

Or use a search engine like Google.

3. Change passwords

After you have checked there are no unwanted email forwarding rules in place, you must:

- change the password for any account that has been hacked
- change the password for any other accounts that use the same password

Look at this guidance for help on how to create strong passwords.

4. Log all devices and apps out of your account

After you have changed your password, you need to sign out of the account on every device you have.

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.

If anyone else tries to log in using your old password, it won't work now.

5. Set up 2-step verification

Many online accounts and services let you set up two-step verification – called 2SV for short.

It means a person must prove who they are in 2 different ways.

Then they can get into online services like banking, email or social media.

Even if a criminal knows your password, they will not be able to get into your accounts if you have 2SV.

2SV usually works by texting or emailing you a number or code that you enter to prove that it is really you.

Setting up 2SV takes a few minutes and makes you much safer online.

6. Update your devices

Do updates to your apps and your device's software as soon as they are offered to you.

Updates are things like:

- protection from viruses
- better changes to your app
- new things

Doing updates is one of the most important things you can do to stop your account from being hacked.

Turn on 'automatic updates' in the settings of your device if it is there.

This means you will not have to remember to do updates.

It is best to update your device at home where you have Wi-Fi.

Keep your device plugged in while it updates.

7. Tell your contacts

If you have been hacked, let these people know:

- anyone you share the account with
- any friends linked to your account if it is a social media account
- anyone who follows your account if it is a social media account

Let them know that you were hacked and tell them they should not trust any recent messages sent from your account.

This will help them to stop being hacked.

8. Check your bank statements and online shopping accounts

Check your online shopping accounts to look for anything bought that you did not buy.

Check your bank accounts for any unusual things bought or money taken.

Contact your bank for more support.

Always use the real official websites or social media channels.

To do this, you can type the organisation name straight into your browser or search engine.

Do not use the links in any messages you have been sent.

9. Who to tell if you have lost money

If you have lost money:

- tell your bank

- report it as a crime to the Police by calling 101

If you are not in Scotland report it as a crime to Action Fraud.

This will help to stop other people being hacked.

If you cannot get your account back

If you cannot get your online account back you will have to start a new account.

When you have done this, give people your new details, and tell them you are not using the old account.

Give your bank, gas and electric companies or shopping websites your new details.

 Prepared by Disability Equality Scotland