

Lead Scotland



How to stay safe when you are online banking



Easy Read



About this document



This is an Easy Read document.



It is about staying safe when you are using **online banking**.



Online banking means using a device like a smartphone or a computer to do things like:

- make payments
- check your account
- ask your bank for help



Online banking is also called cyber banking.



This information comes from Cyber Scotland.

Why we need to stay safe



Lots of people use online banking.



But there are also lots of crimes where other people try to steal our money by reaching it online.

These are called **cyber crimes**.



We must be very careful when we use online banking.

Here are 8 things you can do to stay safe when you are online banking.

1. Find out the latest safety information



Find out what kinds of cyber crimes are happening.



You could go to [Cyber Scotland's website here](#) where they have a new newsletter every month, called a Bulletin.

2. Use really good authentication



In this document, **authentication** means a check that it is really you trying to bank online.



When a bank uses more than 1 way to check it is really you online, it is called **multi factor authentication** - or MFA for short.



This often means that you get sent a special password made of numbers that you have to type in, to show it is you.



If you are offered the chance to set up multi factor authentication, click yes.

3. Keep your software up to date



Software means the instructions and information that tell a computer how to work.



Banks will fix online problems and making their online banking safer.



This information comes to your device in **updates**.

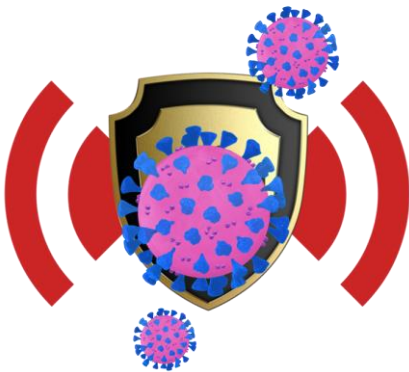


Updates happen when our devices:

- are connected to Wi-Fi
- are switched on
- are not being used – for example at night



Also make sure that you update things like **antivirus software**.



Antivirus software is a program that can:

- find any problem **viruses**
- get rid of any problem **viruses**

on your computer.



A computer **virus** is a bad tool that has been sent to your computer to cause problems.

4. Use safe connections



Think about where you are when you log into online banking.

Try and log on to online banking where you know the WiFi network is trusted and safe.



Try not to use public WiFi places – like cafes, libraries and trains.

This is because **cyber criminals** can sometimes get your information in public WiFi places.



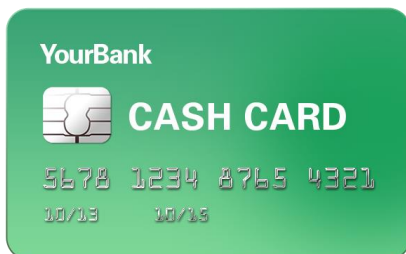
Cyber criminals are people who try to steal other people's information and money online.

5. Be careful of fake messages



Watch out for fake messages that look like they are sent from your bank but are from criminals instead.

This is also called **phishing**.



Phishing messages will try and get you to share your private banking information.



Phishing can happen:

- by email
- by phone call
- by text message



Do not click on any links they show.

Instead, contact your bank by phone or email.

6. Check your account



Check your account often.

Look at your bank statement and check there have been no payments that you do not know about.



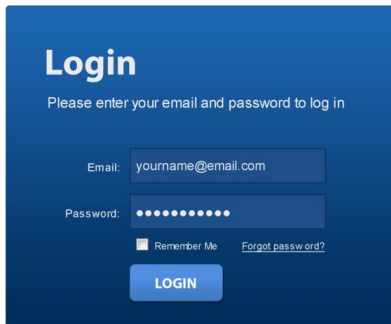
You can set up special reminders called **alerts**.

Alerts will send you a message to let you know if new or unusual payments are made from your bank account.



If you see a payment you do not know about, tell your bank straight away.

7. Use strong passwords



Login
Please enter your email and password to log in

Email:

Password:

Remember Me [Forgot password?](#)

LOGIN

Passwords are the private letters, digits and symbols that we use to get into our online banking.

****Wm63k

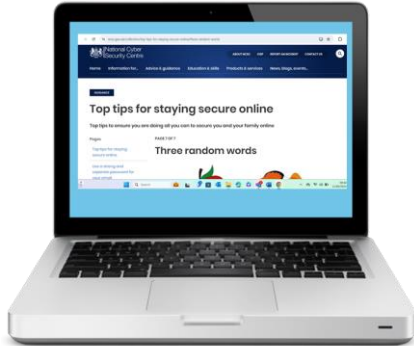


Use a different password for each different bank account.



Make sure the password you choose is strong.

This means that it cannot easily be guessed.



The National Cyber Security Centre says a good way to choose a new password is to put 3 words together that would not normally go together.

You can find out more about using 3 words on [the National Cyber Security Centre website here](#).

8. Keep your devices safe



Devices means all the things that let us get online. Things like:



- smartphones
- tablets
- computers





Try and set up these things on your devices:

- **fingerprint recognition**



This is where you put your finger tip onto a special area of your device and it knows it is you because of the patterns on your finger tip.



- **face recognition**

This is where your device camera sees your face and knows it is you.



- **a strong passcode on your screen lock**

This means a special password of numbers that lets you use your phone.



If someone else picks up your phone, they cannot get past the screen lock if they do not know your passcode.



Do not **download apps** or open **links** from places you do not trust.



Downloading an app means clicking 'install' to get a new app loaded onto your device.



Links are words which can be clicked on to open up a new webpage.



The reason that downloading apps or clicking links can be risky, is because they can have bad things in them which let criminals get into your accounts.

These bad things are called **malware**.

What to do if something goes wrong



If you think something has gone wrong and you might be the **victim** of a cyber crime, do these things below.



A **victim** is the person that something bad has happened to.

Stay calm



Do not panic. Try and stay calm.

Decide what you are going to do next.

Remember that there are lots of organisations to help you.

Let your bank know straight away



Tell them what has happened.

Your bank might be able to get your money back.

Tell Police Scotland



Phone 101 to tell Police Scotland about it.

They will make a report.

The reports help us understand cyber crimes better.

Make your online safety better



Take a good look at the safety tools you are using.

These might be things like:



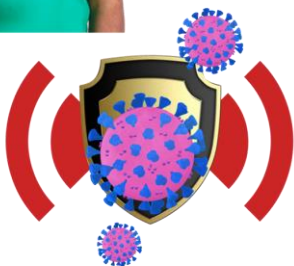
- passwords



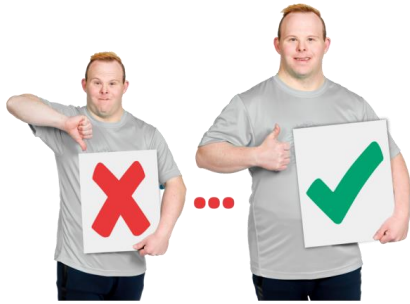
- fingerprint recognition



- face recognition



- antivirus software



Decide if you can make any of these things better.



Or add more things to make your online safety better.

Chat to someone to feel better

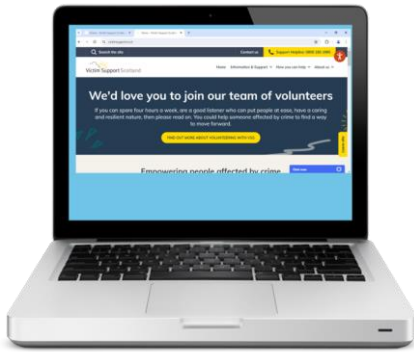


When cyber crime happens to us, we can feel stressed and worried.

Talk to a person or organisation that you trust.



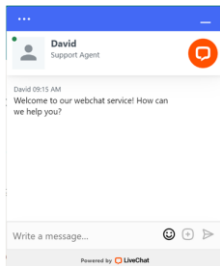
You could talk to someone at Victim Support Scotland.



Click on [Victim Support Scotland's website here](#).



Phone them for free at **0800 160 1985**



Or chat by typing to them in their webchat box.

The webchat box will pop up in the bottom right corner when you go to their website.



Other image credits: Victim Support Scotland / Canva / Cyber Scotland