Lead Scotland

Linking education and disability

Lead Scotland

How to use social media safely

Easy Read

Easy Read made by Disability Equality Scotland

made with photosymbols®

How to use social media safely

Social media is a way to connect with people online and to share information.

Social media includes

- Facebook
- Instagram
- X

X used to be called Twitter.

Social media is a great way to

- stay in touch with family and friends
- find out the latest news

It is important to know how to manage the security and privacy settings on your accounts.

This makes sure nobody else can get your **personal information** like

- your computer passwords
- your bank details
- your birth date
- your National Insurance number

Use 2 step verification to protect your accounts

2 step verification is usually shortened to 2SV.

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

It is a way for **online services** to double check who you are.

Online services are things like

- social media

- banking

- email

Even if someone knows your password they will not be able to access any of your accounts that are protected using 2SV.

Understanding your digital footprint

Your **digital footprint** means all the information that you post online including photos and **status updates.**

A **status update** is a post to let people know what you are doing or to say what is on your mind.

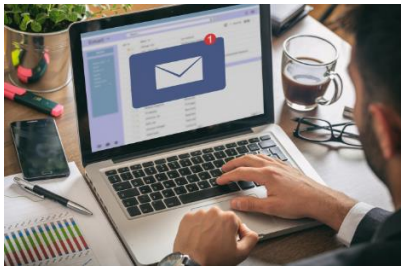
Be careful using social media.

Some people using social media may pretend to be someone else.

Take a moment to check if you know the person, and if the friend, or link, or follow is real.

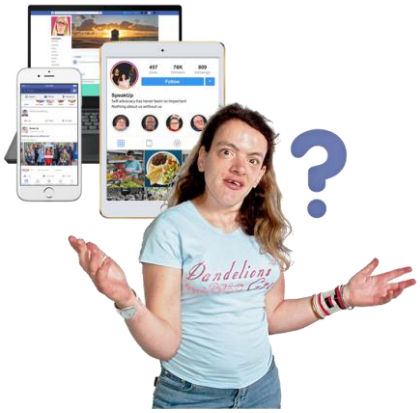
Any information that you put online and do not make it private, can be used by **criminals** to steal your identity, or use it to make **phishing** messages look real.

In this document **criminals** are people who tell lies to steal money from other people.



Phishing is when criminals send emails pretending to be from a company you trust like Royal Mail, or from your bank.

You should think about what you are posting and who can see it.

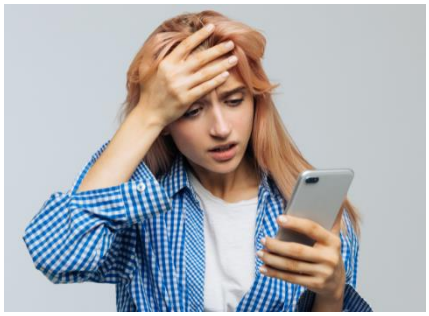


Have you changed the privacy options so that your information can only be seen by the people you want to see it?

You should think about

- what your followers and friends need to know
- what information is not needed, but could be useful for criminals

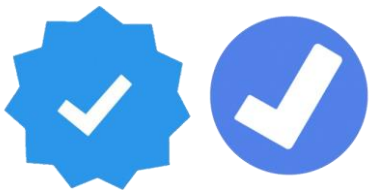
Spotting and reporting fake accounts



A **scammer** is a criminal who will trick you to get your money or personal information.

Scammers make fake accounts and **hack** real accounts to commit crimes.

Hacked means that someone else has got into your system without permission.



Many sites have a way to check accounts, like verified badges for Instagram and Facebook.

This can help to identify real accounts against fake accounts pretending to be a famous person.

Other things to look out for are

- where an account has a date to show when it was set up
- names made up of random letters and numbers like KsBw1935728

- the number of followers – remember that followers can be bought

If a family member or friend posts something that

- does not look or sound right
- does not look like something they would usually post

contact them in another way – for example by phoning them.

Their account might have been hacked.

If their account has been taken over they should follow the National Cyber Security Centre (NCSC) guidance on recovering hacked accounts.

You can report fake posts or accounts to your **provider**.

Your **provider** is the company that provides your internet service.