Easy Read Guide

Based on information from
The Cyber Helpline &
Friends Against Scams

Staying Safe Online

What is cyber crime and how to stay safe

Computers **Phones** **Passwords** **Safety**

58%
of all crimes in England and Wales is online

5M+
People affected in 2025

The Cyber Helpline
Supporting victims of cybercrime

Friends Against SCAMS

1st Enable ltd
Delivering on your potential

What is Cyber Crime?

Cyber crime happens online

People can use the internet, computers or smartphones to try to trick you or steal from you.

Some crime is more widespread through the internet

These crimes can include digital fraud and online harassment and cyber stalking

Anyone can be a target

It does not matter how old you are or how much you know about computers. Cyber crime can happen to anyone

It is never your fault

Criminals use very clever tricks. If you are tricked, it is not because you were silly. It is because they are clever

This guide will help you

You will learn what to look out for and what to do if something goes wrong.

Warning signs to look out for

Unexpected emails or messages

If you get a message you did not expect - especially one asking for money or passwords, be careful. This could be a scam

Asking for your bank details

Real banks will never ask for you for your password or bank PIN in an email, text or phone call. If someone does this - do not give it to them.

They say you must act right now

People may try and rush you so you do not have time to think. It is always okay to stop, take your time and talk to someone you trust

You have won a prize you did not enter

If someone says you have won something you did not enter, it is possibly a trick

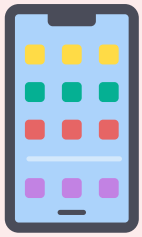
Someone online says they love you very quickly

Be careful if someone you have never met starts asking for money or gifts. This could be a romance scam

Types of scams

Scam emails (phishing)

A fake email that looks like it is from your bank or the government. It tries to get your personal information or get you to click a bad link



Scam texts (smishing)

The same as a scam email but sent by text message. It may say your parcel is waiting or your account has a problem

Scam phone calls (vishing)

Someone calls pretending to be the police, HMRC or your bank. You can always hang up. You will not get in trouble

Romance scams (catfishing)

Someone online pretends to like or love you. After a while they ask for money. Tell someone you trust straight away.

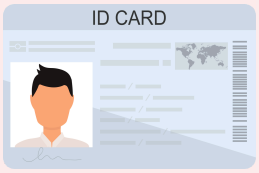
Fake online shopping

Websites that take your money but never send anything. Look for a padlock symbol in the web address before you pay

Types of scams

Account hacking

Someone gets into your social media, email or bank account without your permission. Change your passwords if this happens.



Identity theft

Someone steals your name, details or passowrds to open accounts or buy things pretending to be you

Online bullying and harassment

Someone sends you nasty or threatening messages online. You can block them and report it . You don't have to put up with it

Investment scams

Someone promises you can make a lot of money quickly. They take your money and it is all fake.

Fake job offers

A fake job advert asks for you personal details or money before you can start. Real employers never do this

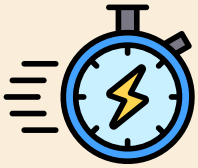
Why do people get tricked?

They make you feel scared or worried

They might say your bank account is at risk or the police are coming. This is to make you panic and act quickly

They make you feel special or loved

They pretend to be your friend or romantic partner to gain trust over time



The rush you

They say you must decide right now. A real bank or organisation will never do this

They seem very trustworthy

They pretend to be the police, HMRC, your bank or even a friend. Always check before you act

Remember

If something does not feel right, stop. Take your time. Talk to someone you trust before you do anything

How to stay safe

Use a **Strong password.** Mix letters, numbers and symbols. Never share it with anyone.

Never share your bank details, PIN or password online, by text or on the phone

If something feels wrong - **stop and ask someone you trust** before doing anything

Do not click links in emails or texts unless you are sure they are safe

You can always **hang up or delete** a message. You never have to respond

Update your phone and computer when it asks you to. Updates help keep you safe

What to do if something happens

If you think you have been tricked, follow these 5 steps straight away:

1. **Stop –** Do not send any more money or share any more details
2. **Change your passwords** on any accounts that might be affected
3. **Contact your bank –** Call the number on the back of your card straight away if money was taken
4. **Report it –** Call Report Fraud on **0300 123 2040** or visit reportfraud.police.uk
5. **Tell someone you trust –** A support worker, family member or carer. You will not be in trouble. It is not your fault

Keep any messages or emails

Do not delete them. They can help police investige what happened.

Who can help me?

Useful contacts

- **Report Fraud:** 0300 123 2040
- **Report Fraud Website:** reportfraud.police.uk
- **Police (non-emergency):** 101
- **Emergency:** 999
- **The Cyber Helpline:** thecyberhelpline.com
- **Friends Against Scams:** friendsagainstscams.org.uk
- **Citizens Advice:** citizensadvice.org.uk
- **Age Uk:** ageuk.org.uk
- **Your support worker**

You are not alone 💙

It is never your fault if someone tries to trick you. You can ask for help. People are here to support you