Skip to main content

How to protect yourself from identity theft

Print this guide

When online, it’s important to take steps to protect your identity so that someone else can’t pretend to be you in order to carry out criminal acts in your name or steal from you.

Unfortunately, there are plenty of online crooks who will try to trick you into giving them your personal information.

This guide will inform you **about all the ways fraudsters will try to trick you into stealing your personal information.**

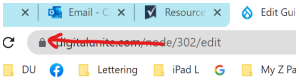
Understanding spyware

Spyware runs in the background of your browser recording your browsing habits, keystrokes , and monitors the programs you use whilst collecting personal data. Whilst your computer is connected to the internet spyware will transmit this personal information to fraudsters. This could be credit card information , usernames and passwords, address books and email addresses.

How to protect yourself from scam, emails, texts and social media messages.

If you are convinced that a message is not legitimate then **do not respond to it**. Avoid clicking on links, opening attachments or downloading software as this could be malware. Also, never log into online banking through a link in a message.

Look out for a secure connection with **https://**, or a small padlock on your browser. This is usually next to the web address on your browser - see where the red arrow is pointing in this screenshot.



In Gmail, for example, you can block unwanted spam email by highlighting the message and filtering it to spam.

Protecting your computer

In the past we have suggested that you use a free online banking security software from Trusteer Rapport. However we have read reports that this can create conflicts with existing security software and so we don't suggest using this now. You can read more about why in this article published by Which Computing and decide for yourself.

We do recommend that you keep your anti-virus software on your computer up to date and always complete security and software updates of your computer system when prompted. Also, if you are in a public space such as a library or coffee shop always keep your laptop and iPad locked with a secure password.

In Windows 10 you can turn Windows Defender SmartScreen on when you're browsing on Microsoft Edge/Internet Explorer. You'll then be notified when you access a phishing website by mistake.

Sharing on social media

Be careful about the information you give about yourself online – for example, when using blogs, forums and social networking sites. Identity thieves may be able to piece together a lot about you just by using public information.

There's more information about identity theft on the Get Safe Online website we also recommend that you follow the advice in our guide 'How to stay safe online'.

Last updated on January 2023

Next steps

- Email safety tips
- How to stay safe online
- Keeping your children safe online
- How to shop safely online

How do digital skills change lives?

Find out about Digital Inclusion