Digital Unite

Inspiring POSITIVE CHANGE through digital skills

How to protect yourself from identity theft

Print

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.

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

Protecting your computer

You can download free online banking security software from Trusteer Rapport. This software will alert you every time you try to log into online banking from an unknown website. We also recommend that you keep your anti-virus software on your computer up to date and always complete security and software updates 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 your browsing on Internet Explorer. You'll then be notifies 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 reccomend that you follow the advice in our guide 'How to stay safe online'.

This guide was last updated on 26/06/2018

Next steps

- Email safety tips
- How to stay safe online
- How to stay safe on Facebook
- Internet safety for kids
- How to shop safely online

Remote Digital Championing!

Guides covering some tips and techniques for providing remote support to learners, an increasingly important service in times of social isolation.

Find out more

Start a Digital Champion movement!

Could your workplace do with developing its digital skills? With funded membership opportunities currently available, now is the perfect time for organisations to join our Digital Champions Network.

Find out more

Subscribe to our newsletter

Join our mailing list to receive the latest news, offers and expert insights from our team.

First name

Last name

Email address

Submit