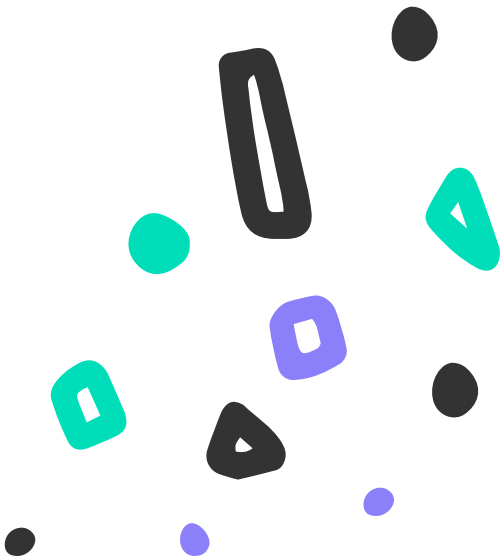
Online Safety



the skills network

Online Safety

In the first half of 2021, criminals stole a total of £753.9 million through fraud, an increase of over a quarter (30 per cent) compared to H1 2020. The advanced security systems used by banks prevented a further £736 million from being taken.*

Using tactics such as scam phone calls, text messages and emails, as well as fake websites and social media posts, criminals seek to trick people into handing over personal details and passwords. This information is then used to target victims and convince them to authorise payments.*

Although this figure is staggering, the fact remains that many of these crimes could have been prevented by a few minor changes in online behaviour.

The Metropolitan Police recently released several short videos to show web users how small changes to their online behaviour can help to protect against cybercrime.

The video clips take just a minute or two to watch, and can help you to protect your finances, personal details and computer security. The purpose of these videos is to show that you do not need to be a computer expert to avoid becoming a victim of online crime – a few good online habits drastically reduce the chances of becoming a victim of cybercrime. To watch the videos, search 'online safety videos from the Metropolitan Police' from your web browser or **click here.**

Good habits to keep you safe online:

1. Find a good password

Ideally, passwords should be more than eight characters long, and contain upper and lowercase letters, and at least one number, letter and special character. When you first log in to EQUAL, you will be asked to create your own password to ensure your account is secure. A good habit to get in is to mix three random words and a memorable date with a special character

2. Always install security updates

Although they can be tedious, security updates occur when the developer notices that a part of the software is vulnerable and could provide an opportunity for cybercrime. For example, some software updates prevent bugs that cause your internet browser to crash, which can be disruptive when you are working. EQUAL autosaves every three seconds, so any work that you complete should not be lost. However, installing updates should also stop this from happening.

3. Be careful when using unsecure Wi-Fi

Online shopping, banking, and sending sensitive documents using a public Wi-Fi can make it easy for criminals to intercept your information. We handle the information you share with us very carefully. It is a good idea to use a Virtual Private Network (VPN) if you are using a public Wi-Fi and sending us any personal information to ensure that this cannot be accessed by anyone else.

4. Be suspicious of emails from unknown senders

Phishing is the practice of sending fake web links via email to trick someone into downloading an attachment that can allow criminals to access your personal information. Never click on a link from an unknown sender, and always be wary of contact details sent to you via email. Use the contact details that are advertised on official websites rather than the ones sent in the body of a message – you can check our contact numbers against the ones advertised on our website, so that you can be sure it is us contacting you.

Online safety and British Values

There are many British laws that exist to protect people online - for example, the Computer Misuse Act (1990), which relates to unauthorised access to others' computers, usually with the intent to cause damage. This important law, amongst others, plays a vital role in underpinning British Values. Living under the rule of law protects individual citizens and is essential for their well-being and safety.

The 4Cs

There are numerous issues within the topic of online safety and whilst these are vast, they can be categorised into four main areas of risk. These four areas are known as the '4Cs'*:

1. Being exposed to illegal, inappropriate, or harmful **content**. This could include pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.

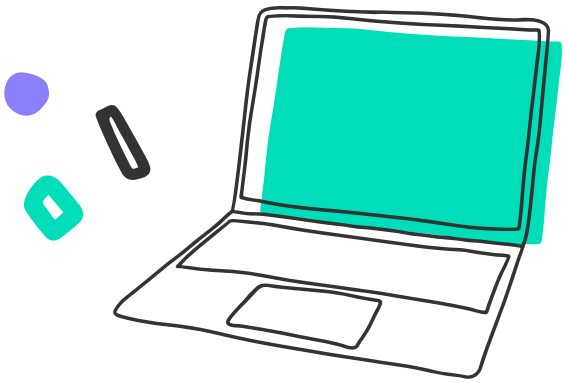
2. Being subjected to harmful online **contact** with other users. For example - peer pressure, adults posing as children with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

3. Personal online **conduct** that increases the likelihood of, or causes, harm. This may involve making, sending and receiving explicit images (e.g consensual and non-consensual sharing of nude and semi-nude images or videos) and/or pornography, sharing other explicit images, inappropriate use of location services and online bullying (cyberbullying).

4. **Commerce or Contract** – this relates to financial risks such as online gambling, inappropriate advertising, phishing and/or financial scams, along with 'accepting' the terms and conditions of certain online contracts without having full knowledge or understanding prior to doing so.

***https://saferinternet.org.uk/guide-and-resource/what-are-the-issues**

Online abuse is defined as any abuse that takes place online and can happen across any device that's connected to the internet, such as mobile phones, tablets, and computers. Online abuse can happen anywhere online, including social media, text messages and messaging apps, emails, online gaming, online chats, live-streaming sites, or other channels of digital communication. For further information, guidance or support please see the links listed on the last page of this document.



Digital Resilience

One of the key concepts when remaining safe online involves creating a resilience to online risks, meaning you are able to recognise and manage the risks you come across when you socialise, explore or work online.

'Digital resilience involves having the ability and awareness to understand when you are at risk online, knowing what to do if anything goes wrong, learning from your experiences of being online, and being able to recover from any difficulties or upsets.'

(Source: Digital Resilience Working Group, The UK Council for Child Internet Safety)

Understand

An individual understands when they are at risk online and can make informed decisions about the digital space they are in

Know

An individual knows what to do to seek help from a range of appropriate sources

Learn

An individual learns from their experiences and is able to adapt their future choices where possible

Recover

An individual can recover when things go wrong online by receiving the appropriate level of support to aid recovery

(Source: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/831217/UKCIS_Digital_Resilience_Framework.pdf)

Online Safety

We hope you found this update helpful. If you need any support, advice or guidance, please do not hesitate to get in touch with us using the details provided at the bottom of this document.

We would strongly encourage you to explore the following links for further information and resources around keeping yourself and your loved ones safe online:

- **https://www.ncsc.gov.uk/section/information-for/individuals-families**
- **https://www.met.police.uk/advice/advice-and-information/fa/fraud/online-fraud/cyber-crime-fraud/**
- **https://sharechecklist.gov.uk/**
- **https://www.internetmatters.org/advice/**
- **https://www.thinkuknow.co.uk/**

Kind regards,

The Skills Network

***Source: ukfinance.org.uk**

Get In Touch

T: 01757 210022
E: sales@theskillsnetwork.com
W: www.theskillsnetwork.com