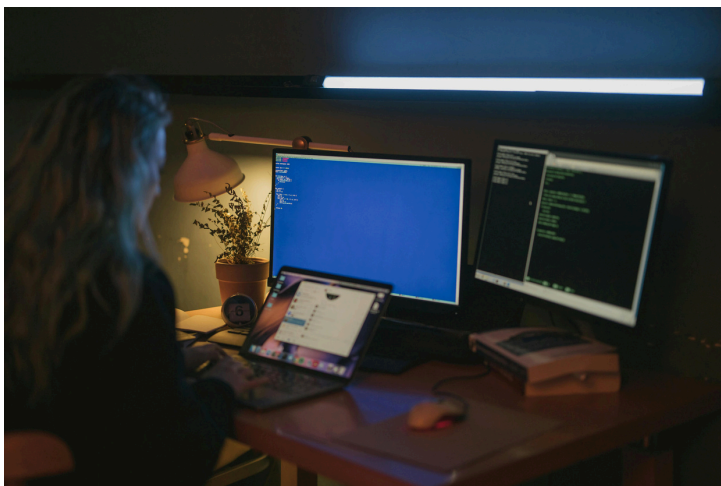




SAFEGUARDING

OUR BI-MONTHLY SAFEGUARDING NEWSLETTER

JUNE, JULY 2024 • ONLINE SAFETY



WHAT'S INSIDE?

In our latest issue we will be discussing online safety and what this can include. Also we will discuss what has caused the rise in this issue and what you can do to stay safe.

If you require further support, please see the links on the last page of the document.

INTRODUCTION

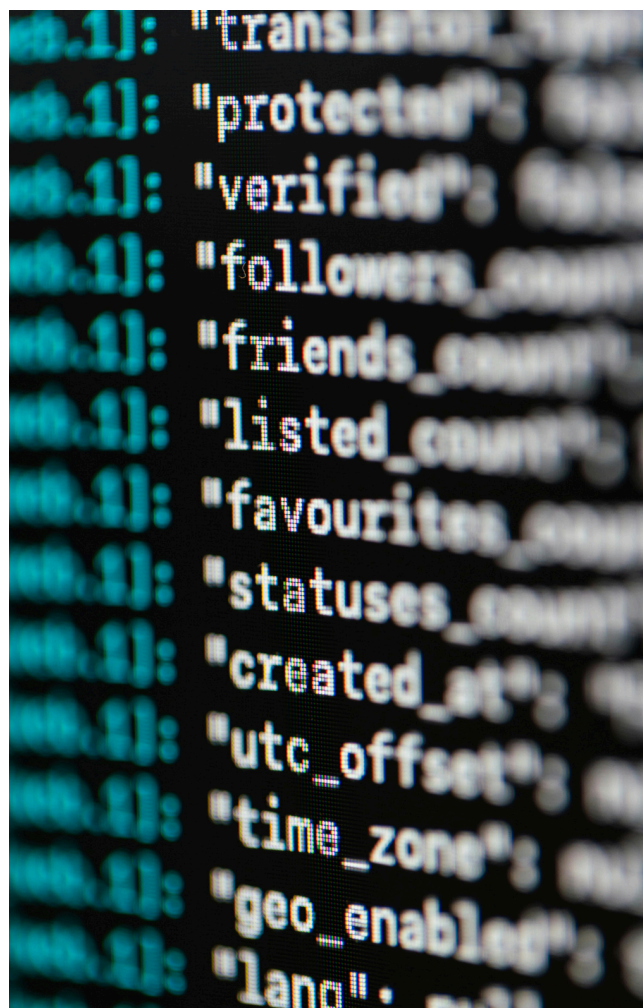
Online Safety, also known as e-safety and cyber safety, refers to the act of staying safe online. Online Safety encompasses all technological devices which have access to the internet, from PC's and laptops to smartphones and tablets.

Essentially it's having the ability to recognise and understand **threats** that exist on the internet, as well as having the skills and knowledge to **avoid** them all together.

WHY HAS THIS INCREASED?

Several factors contribute to the increase in **importance** of online safety, a select few of these are:

- Increased Internet Usage - this is mainly due to Covid 19 and its remaining impact. By this I mean that, working and learning from home increased and has remained that way totalling **44%** of the population to now still be remote.
- Social media - There has been a rise in social media accounts plus more and more social media platforms either popping back up or being discovered. The anonymity and reach of the internet and vast array of platforms makes it easier and more common for individuals to be **cyberbullied**, which then has a domino effect for mental health concerns, such as anxiety, depression, suicidal thoughts etc...
- Privacy and Data Security - Recently, there has been an increase in high profile data breaches and privacy scandals which has subsequently raised concerns about the **protection** of personal information online.





TYPES OF ONLINE THREATS

Online threats come in various forms targeting individuals, businesses and organisations. Understanding different types of threats allows you to be more prepared for if you were to face one,

Some examples are:

- **Malware** - Viruses, Trojan, Worms, Ransomware, Spyware,
- **Phishing** - Email phishing, Spear phishing, Smishing, Vishing,
- **Credential Stuffing** - Using stolen usernames and passwords from one service to gain access to accounts on other services, exploiting users who reuse credentials.

As well as these there are many more threats, by understanding them it can help you to **mitigate** threats and risks, ultimately protecting your digital assets and personal information.

If you happen to **suffer** from one of these threats, you can visit one of these websites on ways to **resolve** the problems and understand what to do next:

- <https://www.verywellhealth.com/covid-19-online-harassment-5084544#:~:text=5%20Steps%20You%20Can%20Take%20If%20You%27re%20Being,...%20%20Realize%20This%20Isn%27t%20About%20You%20>
- <https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime>
- <https://us.norton.com/blog/how-to/how-to-recognize-and-protect-yourself-from-cybercrime>
- <https://www.police.uk/advice/advice-and-information/fa/fraud/online-fraud/cyber-crime-fraud/>

SEXUAL EXPLOITATION

If you suspect sexual exploitation please talk to the **designated safeguarding team**. If it is an emergency always contact **999**.

MODERN SLAVERY

If you suspect modern slavery or human trafficking please report it to the designated safeguarding. If there is immediate danger always call 999.

RADICALISATION

If you are worried that someone is being radicalised please contact the police on 999.

If you are concerned that someone is being radicalised in your workplace, and there is no immediate danger, please talk to the prevent lead.

COUNTY LINES

You can speak to your local police by dialling 101, or in an emergency 999.

If you suspect someone is being exploited please talk to the **designated safeguarding team**

SCAMMING

If you think that you've been scammed, you should report the crime or incident to **Action Fraud**, not your local police service (unless it is an emergency). Action Fraud will initiate any necessary police investigation into your loss.

BLACKMAIL

If you suspect blackmail please talk to the **designated safeguarding team**. If it is an emergency always contact **999**.

FRAUD

If you think that you've already experienced fraud, you should report the crime or incident to **Action Fraud**, not your local police service (unless it is an emergency). Action Fraud will initiate any necessary police investigation into your loss.

MATE CRIME

If you think that someone is taking advantage of you or someone you know: speak to the designated safeguarding team or someone you trust, **do not** tell the person who is pretending to be your friend.

OUR SAFEGUARDING TEAM

Contact Steadfast Training's Safeguarding team on 0845 223 2401 or email safe-guarding@steadfasttraining.co.uk

Our Safeguarding Officers

Robert Wright - 07985338185
Alison Law - 07720092609
Chloe Robinson - 07985338116

[Report a Safeguarding Issue](#)



9 PROTECTED CHARACTERISTICS

- Age
- Disability
- Gender
- Reassignment
- Marriage & Civil Partnership
- Pregnancy & Maternity
- Race
- Religion or Belief (including lack of belief)
- Sex
- Sexual Orientation

PREVENT DUTY

The Prevent Duty is part of the government strategy to reduce the risk of Extremism, Terrorism and Radicalisation.

[View our Prevent Leaflet](#)

Report possible terrorist activity online If you are concerned about someone or see anything suspicious call the local police or the police anti-terrorist hotline on 0800 789 321.

BRITISH VALUES

British Values are defined as;

- Democracy
- The Rule of Law
- Individual Liberty
- Mutual respect for and tolerance of those with different faiths and beliefs and for those without faith.