SAFEGUARDING

OUR BI-MONTHLY SAFEGUARDING NEWSLETTER

SEPTEMBER - OCTOBER 2021 • CYBER SECURITY & CRIME

WHAT'S INSIDE?

In our latest issue we will be covering the topic of Cyber Security and how you prevent yourself from falling a victim of cyber crime.

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

WHAT IS CYBER SECURITY AND CRIME?

Cyber security is a collection of technical controls and human protocols, which are designed to protect organisations and individuals from the actions of criminals.

Cyber-crime is a way of committing crimes via computers and their networks. This may be to steal people's identities or business secrets, to commit fraud or for other exploitative or malicious purposes.

There are two overarching areas of cybercrime:

- cyber-dependent crimes - which can only be committed through the use of online devices and where the devices are both the tool to commit the crime and the target of the crime, and
- cyber-enabled crimes - traditional crimes which can be increased in scale by using computers.

IMPORTANT INFO

These crimes take on a number of different formats - from hacking and use of the dark web to trolling on social media and phishing or identity thefts.

Cyber Crime is one of the fastest growing criminal activities across the world, and can affect both individuals and businesses.

TYPES OF CYBER CRIME

Cyber crime is a global threat. Several million cases of fraud and of computer misuse are reported to the police every year. Between April 2018 and March 2019 there were:

- 741,123 crimes were reported to Action Fraud.
- £2.2bn lost by victims.

Cyber crime, covers all crimes that take place online, are committed using computers, or are assisted by online technology

Types of Cyber Crime

- **Hacking** is the unauthorised use of or access into computers or networks by using security vulnerabilities or bypassing usual security steps to gain access.
- **Malicious software** - or malware - can be spread between computers and interfere with the operations of computers. It can be destructive, causing system crashes or deleting files, or used to steal personal data.
- **Distributed Denial-of-Service (DDOS)** attacks are where more than one, and often thousands, of unique IP addresses are used to flood an internet server with so many requests that they are unable to respond quickly enough. This can cause a server to become overloaded and freeze or crash, making websites and web-based services unavailable.
- **The dark web** is made up of a number of untraceable online websites. Specific software and search engines must be used to access the websites.

Social media offences

- **Trolling** is a form of baiting online which involves sending abusive and hurtful comments across all social media platforms.
- **Online threats** could take many forms including threats to kill, harm or to commit an offence against a person, group of people or organisation.
- **Disclosure of private sexual images without consent –** so called "revenge porn" is a broad term covering a range of activity usually involving an ex-partner, uploading intimate sexual images of the victim to the internet, to cause the victim humiliation or embarrassment.
- **Online harassment** can include repeated attempts to impose unwanted communications or contact in a manner that could be expected to cause distress or fear.
- **Grooming** refers to the actions of an individual who builds an emotional connection with a child to gain their trust for the purposes of sexual abuse or sexual exploitation.
- **Stalking online** is a form of harassment which can involve persistent and frequent unwanted contact, or interference in someone's life

Cyber-enabled fraud

Fraudsters use the internet to gain sensitive personal information through phishing attempts. Often criminals pretend to be a company and trick a victim into using a malicious website or installing malware on their device. A phishing attempt can be sent to a range of 'targets' at the same time.

- This can lead to **identity theft** - criminals gathering enough information about a victim to take their identity and commit fraud.
- Criminals can also use the internet to carry out **intellectual property fraud** - creating counterfeit goods to sell online, either billed as genuine or clearly fake, or setting up and running websites purporting to be genuine retail outlets.

INFORMATION FROM:HTTPS://WWW.CPS.GOV.UK/CRIME-INFO/CYBER-ONLINE-CRIME

HOW TO PROTECT YOURSELF

The National Crime Agency have stated most cyber attacks could be prevented by taking these basic security steps:

- **Choose strong passwords** and don't reuse them for multiple logins
- **Install security software** such as anti-virus and two-factor authentication. This kind of software is often available for free.
- **Keep all security software and operating systems updated** (this can be set to update automatically)

To further protect yourself online the Met Police have released a list of measures you can take to reduce your cahnces of becoming a victim.

- Try using three unrelated words, eg fishbooktable; and think of three different words for each account, so if one is compromised the others are safe
- Never give personal or sensitive details out online or over email
- Only download from legal, trusted websites
- Only open emails and attachments from known and trusted sources
- Only ever use websites that start with https://, however make sure that you're on the correct site by sense-checking the full website address
- Ovoid using public WiFi hotspots that are not secure, use your 3/4G data. If you have no choice but to use Public WiFi, then only use it with a Virtual Private Network enabled on your device
- Regularly back up your data
- Control your social media accounts – regularly check your privacy settings and how your data is being used and shared
- Be cautious of internet chats and online dating – there's no guarantee you're speaking to who you think
- Be extremely cautious if you're asked for money

REPORTING CYBER CRIME

If you are currently being subjected to a live and ongoing cyber-attack then please **contact the Metropolitan Police on 101**.

If you suspect you've been scammed, defrauded or experienced cyber crime, the Action Fraud team can also provide the help, support and advice you need.

ActionFraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040

Call Action Fraud on 0300 123 2040 (textphone 0300 123 2050).

You can contact Citizen's Advice to get advice from a Scams Action adviser by calling **0808 250 5050.**

Scams advisers can help you if;
- think you might have found an online scam
- need advice about scams
- want to report an online scam

We'll let you know what to do next, and give you support on the issues you might be facing.

citizens advice

The service is open from Monday to Friday, 9am to 5pm. We're closed on bank holidays.
Calls are free from mobiles and landlines.

INFORMATION FROM:HTTPS://WWW.CPS.GOV.UK/CRIME-INFO/CYBER-ONLINE-CRIME

FURTHER SUPPORT & INFORMATION

National Cyber Security Centre
The NCSC's cyber security advice to protect you and your family, and the technology you rely on.

Metropolitan Police
Met.Police.UK have put together useful advice and informative videos

Cyber Aware
Essential advice on protecting yourself online

Action Fraud
Action Fraud is the UK's national reporting centre for fraud and cybercrime where you should report fraud if you have been scammed, defrauded or experienced cyber crime in England, Wales and Northern Ireland.

0300 123 2040 Monday to Friday 8am - 8pm or Report online

If you or someone else is in immediate danger or risk of harm dial 999

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.

OUR SAFEGUARDING TEAM

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

If you wish to raise an issue of safeguarding for a learner or individual related to Steadfast Training Ltd in any way, please contact the centre immediately on: 0845 223 2401.

Report a Safeguarding Issue

For more information on anything covered in the newsletter, feedback or ideas for the next issue, please contact us on chloe.robinson@steadfasttraining.co.uk.