What are Cybercrimes

The term 'cybercrime' is used to refer to a broad range of behaviours online that are considered to be illegal and could get someone into trouble. Cybercrimes can be harmful to those involved in the behaviour ('perpetrators') and those impacted by the behaviours ('victims'). Those involved also risk getting into trouble with the police and could face prosecution.

What leads someone to commit crimes online?

Criminal behaviours are very interconnected, meaning if someone is involved in one form of illegal behaviour either online or offline, they are likely to be involved in other forms of crime. It's also important to know that taking risks online is related to online crime. Risky behaviours, behaviours which are harmful but not necessarily illegal, can lead to involvement in cybercrime. For example, accessing certain dark web forums can lead to the risk of young people being recruited into money laundering schemes and other forms of fraud and theft online. There are many different reasons why someone ends up committing crimes online. It's important to know that there are different motivations behind different cybercrimes - for example sexual abuse, hacking or identity theft can all be used to harass someone online.

What can I do to reduce the risks?

Try to avoid or reduce the following risks related to harmful and illegal behaviours online:

- ✓ Spend less time online or on digital devices
- ✓ Keep devices out of reach overnight or when sleeping
- ✓ Avoid use of certain social media platforms that contain potentially harmful content
- ✓ Reduce the number of accounts and platforms used on social media
- ✓ Try to avoid interacting with accounts (e.g., by blocking or muting) that contain harmful content on social media
- ✓ Be careful of using of online spaces that are potentially more risky than others (like dark web forums or certain types of chat rooms)
- ✓ Only do things online that you would be OK with offline
- ✓ Try to avoid taking risks, acting on impulse, or doing harmful things online
- ✓ Avoid doing things online that are hurtful to others or could get you into trouble
- ✓ Think carefully about friendships with those who do things that are harmful or illegal, either online or offline
- ✓ Improve your knowledge of online safety and security, and find out what behaviours online might be criminal
- ✓ Do not do things offline that are illegal as this is one of the main risks associated with committing online crimes

Cybercrime Behaviours

Hacking

Hacking is defined as attacks against data and systems by illegal access, interference, and interception. For example, stealing information, hacking someone's social media account, as well as the use of viruses and malware.

Financially motivated crime

Theft or attacks against property which can include fraud, forgery, identity theft, phishing, and piracy.

Money Muling & Illegal Marketplaces

Behaviours ranging from not very technical (like letting someone use your bank account to transfer money) to very technical (like using illegal virtual marketplaces or dark web markets).

Online Sexual Crimes & Harms

Attacks against individuals, everyone can be targeted however females are more likely to be targeted. Often the motive is to upset, humiliate, or intimidate. Including extortion, stalking, and abuse.

Online Hate

Attacks against groups, often the motive is related to extreme hate towards a gender, identity, sexuality, culture, or religion. Including hate speech and even terrorism.

Online Harassment

Attacks against individuals, often the motive is to upset, humiliate or intimidate someone. Including, extreme harassment and blackmail or extortion.

University of East London

ICC

CC-DRIVER

For Safer Internet Day 2023, from the CC-DRIVER Project partners at The University of East London, Institute for Connected Communities. This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883543.