SOUTH WEST POLICE
RCCU
Regional Cyber Crime Unit

CYBER CHOICES

Cyber Choices and the SWRCCU

What we do

We offer interventions for young people who are at risk of being involved with cyber dependent crime. We can do this on a 1:1 basis, as a workshop or more long term interactions. We explain the ethical and legal aspects of cyber as well as promoting the positive use of it (such as in careers).

What is cyber dependent crime?

Basically, any crime that can only be committed with the use of technology (e.g. hacking without permission). A 2015 NCA study showed that the average age of suspects and arrests in cyber crime investigations was 17 years old.

What to look out for

Certain behaviours may indicate risk, these could include spending large amounts of time on computers, and tech related online forums. Be aware of social difficulties (e.g. being isolated, ASD), and take note of any technical language used such as those described on the next page.

Please note that we are not saying these are definitive indicators directly resulting in criminality, they are behaviours which are often exhibited by subjects we've encountered.

When should you refer to Cyber Choices?

If any of the above apply, or if you have an incident such as a young person interfering with devices or networks, or accessing online accounts without permission. If you are unsure, feel free to email us and we will help in any way we can. Our aim is not to criminalise, and we will treat any concerns confidentially and discreetly.

How can we support the young person and their care givers?

You can signpost them to the resources on the National Crime Agency website, or you can arrange to have a meeting (online or in person) with us, where we can discuss and establish a course of action. Please note, we cannot work with a person if they are under investigation for a criminal case. We can revisit this once the case is closed.

Contact us at: SWCyberPrevent@avonandsomerset.police.uk

swrocu.police.uk/cyber

SW Regional Cyber Crime Unit

@swrccu

The Computer Misuse Act 1990

Section 1

Unauthorised access to computer material.

- You watch your friend ener their username and password. You remember their login details and without their permission, later log in and read all their messages.

Section 2

Unauthorised access with intent to commit or facilitate commission of further offences.

- Your friend leaves their tablet on the sofa. Without their permission, you access their gaming account and buy game credits with the attached credit card.

Section 3

Unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer.

- You are playing an online game with a friend who scores higher than you. You use a 'Booter' tool knowing it will knock them offline, so you can win the game.

Section 3ZA

Unauthorised acts causing, or creating risk of, serious damage.

- You hack in to a police network. This results in delays to emergency calls and even though it was not your intention, you were reckless in your actions.

Section 3A

Making, supplying or obtaining articles for use in offence under section 1,3, or 3ZA.

- You download software so you can bypass login credentials and hack into your friend's laptop, however you've not had a chance to use it yet.

Glossary

Black hat: A hacker who illegally hacks for a variety of reasons, including for the challenge or to benefit themselves.

Booter: Used to launch a Denial of Service (DDoS) attack. Also known as a stressor.

Denial of Service (DoS): An attack involving the bombarding of a website or web service (such as email) by sending it multiple requests. If these come from multiple devices it is 'Distributed' (DDoS).

Virtual Private Network (VPN): Software which creates an encrypted online connection to another network or system. It can also be used to mask the origin or location of the user.

More terms and information can be found online through the National Crime Agency (NCA) online, and through Cyber Choices leaflets.