V1.0

rocu south east
Regional Organised Crime Unit

Cyber Choices
◆ Delivery Notes ◆

Key Stage 3

Years 7 & 8

Why Teach the Computer Misuse Act?

Teens more likely to hack (5%) than smoke (3%) or have sex (2%) [1]

Teens more likely to hack (5%) than be in a gang (2%) [1]

1 in 4 Teenagers admitted having tried to compromise someone's account [2]

~1% of teenagers sent a virus at least once in previous 12 months [1]

17 Average age of arrest for cybercrime [3]

61% Of hackers started before 16 yrs old [3]

✓ This is a Safeguarding Issue for Education

✓ This is an Ethics and Online Harms subject

[1] Risky behaviours - Centre for Longitudinal Studies – UCL January 2018

[2] Tufin Teenage Hacking Habits

[3] NCA / CREST Pathways into Cyber Crime

The latest version of all material required is always available at:

https://serocu.police.uk/champions/

Why teach about cybercrime?

Cybercrime is one of the fastest rising crimes in the UK, and is particularly common among young people, with 61% of hackers beginning hacking before the age of 16, and with some becoming involved with illegal online activity as young as 12. Research from the National Crime Agency (NCA)[3] suggests that young male gaming enthusiasts are most likely to be involved, mapping a progression from becoming interested in coding, to carrying out modifications to computer games. This can quickly lead to accessing online coding or hacking forums, where gradually the idea of accessing or stealing certain pieces of information is introduced. They may then be identified by individuals or groups involved in cybercrime who encourage them to participate in illegal online activities.

The concern is that many young people are not aware of what activity is or isn't illegal online, or assuming that their actions are 'victimless crimes' when in fact there can be very serious consequences for both individuals and businesses.

Creating a safe learning environment

It is essential that students have the right learning environment in order to get the most of the lesson, including feeling able to share ideas without criticism, negative comments or bullying. The opportunity should also be given to make disclosures in private and the right setting allows the teacher to manage discussions.

If you are a STEM Ambassador: it is the teacher's responsibility to safeguard the students, but you can contribute by creating the right learning environment, including laying down some ground rules:

- Everyone has the right to speak and be heard with respect from others
- Everyone should be careful to use the right language which must not be offensive
- People should use the right phrases or terms and ask if they do not know
- If you wish to add comment to a point, statement or opinion from someone else, your comment should be on *what* was said and not *who* it was said by
- Nobody should share anybody else's personal experiences and should be very cautious about sharing your own (this can lead to uncomfortable or distressing disclosures)
- Nobody should be put on the spot
- There should be no assumptions or judgements about anybody

You should consider the need or desire for an anonymous comment box for questions or feedback, to avoid anyone having to voice them in front of the class.

You should consider the differing needs and experiences of individuals in the class – some may have experience of being the perpetrator or victim of some of the crimes described. While the harm is generally not physical it may be connected with other offences such as cyber bullying. Seek guidance from a safeguarding lead or teacher as necessary.

STEM Ambassadors: the teacher has a responsibility to ensure compliance with the school's policies on safeguarding and confidentiality. You should turn to them for guidance.

Finish the lesson ensuring that everyone knows that more guidance or help can be sought if necessary. Explain that there are professionals that the teachers can turn to for expert help.

Differentiating learning for those with SEND

Teachers are best placed to decide how the needs of specific students may be met differently and it is impossible to provide comprehensive guidance. The modular nature of the lesson plan has been designed to provide different possibilities to suit the audience and environment.

The lesson has been designed for all but specific consideration given to those with autistic spectrum disorder (ASD) who are anecdotally more vulnerable to becoming involved in cybercrime. The lesson avoids trying to focus too much on emotional aspects or on creating a model which suggests that there is a greater financial benefit to being a cybercriminal. For more advice on teaching those with ASD seek specialist help from the National Autistic Society.

Glossary of terms

There are lots of potentially confusing terms in the cyber world and it is important to have a good grasp of these terms to speak with confidence. Precise use of language can avoid misconceptions and ambiguity.

Term	Meaning
Shoulder surfing	Looking over somebody's shoulder while they type in their password or PIN code so that you can remember them and use them later to login to their account – this is NOT illegal until you use the details to actually login and do something with the other person's account
Denial of Service (DoS) *aka* 'Booting' or 'Stressing'	Knocking someone else's internet connection out by overwhelming it with thousands or millions of tiny data requests every second. While it sounds very technical it is widely experienced in online gaming where it is easy for players to find their opponent's IP address (their online address) to target. There are illegal websites providing DoS services called webstressers or web-booters for a matter of a few pounds per attack and many even accept PayPal. You may hear of 'Distributed Denial of Service' or DDoSing which is where thousands of virus infected computers or devices perform the attack. These are very hard to defend against. The maximum penalty for performing a DoS attack in the UK (against anywhere in the world) is 10 years in prison (Section 3 Computer Misuse Act).
Hacking	Hacking is a neutral term that is generally regarded as bad because of how the media and Hollywood portray hackers. This puts many off of the positive side because of stereotypical images of hoodies in front of green screens. Hacking involves trying to defeat the cyber security of a system. With permission this is a well-paid career – ethical hacking. Without permission this would usually be unauthorised access to computer material (Section 1 Computer Misuse Act) with a maximum penalty of 2 years in prison, or 5 years in prison if you intended to commit another offence once you had hacked your way in (such as stealing money or committing a fraud).
Firewall	A security system which regulates what internet traffic can come into or go out of a computer or network. In theory, it prevents bad stuff coming in from the public internet but still allows good traffic such as internet browsing, but they are not intelligent and can be circumvented by users doing the wrong thing. Most internet enabled devices have a firewall of some sort including mobile phones, tablets and laptops. On a computer network (like the school) there will dedicated IT devices providing the firewalls.
Hacktivism	Misusing computers or networks to make a political, social or economic point – activism online. Some move from simply broadcasting opinions into breaking the law. Defacing websites is quite common, as are Denial of Service (DoS) attacks.
Malware	**Mal**icious Soft**ware**, which to most of us means a computer virus. There are in fact many different types of malicious software including viruses, worms, rootkits, trojans… and all of them do bad things to computers or networks in different ways.
Remote Access Trojan (RAT)	Like the story of the Trojan horse, this is software that pretends to be legitimate – often antivirus software. In reality, once installed, a RAT creates a 'back door' to the machine or network allowing cyber criminals unlimited access to whatever the logged-in user has.
Mods *aka* Modding and Cheats	'Modding' a computer game means changing the code in some way so that the player can do something the author of the game did not intend. Some games (i.e. Minecraft) actively encourage modding. Cheating is entering codes or taking advantage of a bug (error) that then allows the player to do something. Both typically let players fly, or unlimited ammo.
Black Hat / Grey Hat / White Hat Hacker	Hacking (as above) is a neutral term. A White Hat Hacker is one who has permission and is paid to hack to test cyber security defences. They stay legal. Black Hat Hackers happily break the law and usually do. Grey Hats sit in between – they try to be legal but revert to crime sometimes such as when they are disgruntled.

Term	**Meaning**
Ransomware	A form of malware (see above) which, once on a computer, uses encryption to prevent the user of the computer from accessing some or all of their files. The cyber criminal then leaves a message which asks the user to pay a ransom – often in Bitcoin or other cryptocurrency (see below) to release the files back to the user. The reality is, paying rarely gets the files back. This is one of the most dangerous but common forms of malware at the moment and has taken out a number of schools across the UK.
Bitcoin or Cryptocurrency	Bitcoin was the first mainstream cryptocurrency. Cryptocurrency, despite being called currency, is NOT legal money like the pound is as there is no Government or other recognised body controlling the currency. The UK state it should be considered more like an asset with a value, only a virtual asset. The price goes up and down based on how many people are buying and selling them at any one time. They are built around the concept of a 'blockchain' which is a long record of all sales and purchases. New Bitcoins (and others) are said to be 'mined' (created) by solving complicated mathematical equations. The first to solve the next equation gets the next Bitcoin (etc). Another common cryptocurrency is 'Ethereum'.
The Dark Web	The internet can be split into three tiers: • The Surface Web – the bit of the internet that can be found using a simple Google search… publicly accessible and searchable • The Deep Web – most of the internet exists here… this is computer networks connected to the internet but you need permissions or knowledge to get access. Google cannot index this to search it • The Dark Web – created by the US Navy originally to allow secure communications back from abroad, these websites need special addresses and special software (The Onion Router, or TOR) to get to it. Multiple layers of encryption (like the layers of an onion, hence the name) provide a degree of anonymity. As a result, cyber criminals have taken up shop on the Dark Web in large numbers selling everything from guns, drugs and indecent images of children to cybercrime services, malware and stolen personal data. There *is* legitimate use of the Dark Web (some estimates as high as 50%) but finding legitimate uses is harder than finding illegal or questionable content. **Answer to a common question: No, it is NOT illegal** to access the Dark Web. Telling young people not to go there only leads to mystery and them visiting it anyway. Explaining that it is not illegal but is full of horrible, often illegal content and that nobody can be trusted there is more effective. Western Governments, Law Enforcement and academics (usually universities) control the majority of the TOR 'nodes' (servers to which you connect), which means in reality Police are becoming quite effective at catching cyber criminals on the Dark Web and it is not as anonymous as perceived.

Getting Support

Common Questions

We attach a list of questions we encounter frequently to the resources. Please share any you receive and CAN answer with us so we can update this list.

Questions you cannot answer

If someone has a specific question that you cannot answer it is important that we try to resolve the query. Explain that you are not sure but you know people who will. Agree that you will find out and contact their teacher to share the answer. Ideally, have the conversation jointly with their teacher, but if necessary take their first name only. Contact us and we will share the answer with you and the school.

Concerns about a specific pupil

There will be times that a specific pupil may show an aptitude to this world and this should clearly be encouraged. Highlight the pupil to teaching staff just in case they missed the signs. There are lots of extra resources for individuals on our website.

On the other hand, there will be some pupils whose language, behaviour or interests make you concerned they are getting it wrong in this space. Please share these concerns with the teaching staff and encourage them to get in touch with the Cyber Choices team. Please emphasise that our aim is to support and divert and avoid unnecessary criminalisation of young people. We want to reach them before it is too late!

There is a contact form on our website under:

https://serocu.police.uk/cyber-choices-educator/

or you can pass on our email address: CyberChoices@serocu.pnn.police.uk