



CYBER CRIME WORKSHOP

EDWARD WILSON PRIMARY SCHOOL

29TH SEPTEMBER 2025

A brief history

The Computer Misuse Act 1990 was introduced into UK Law after two hackers obtained, without the persons knowledge, the username and password of an I.T. engineer who worked for a large telephone communications company.

The two hackers then remotely logged into the I.T. engineers' account and to their surprise they were able to access the mailbox of Prince Phillip! The police were notified and the hackers were arrested. The two hackers were convicted under the Forgery and Counterfeiting Act 1981. The hackers claimed that their actions were not for financial gain, but they had simply wanted to demonstrate that they could hack the system.

On appeal, their convictions were overturned as it could not be said that they had committed forgery under the legislation. The Computer Misuse Act 1990 was created to deal with the issue of accessing or modifying data without permission.

HACKING IT LEGAL



THE COMPUTER MISUSE ACT 1990

Get to know the legal
boundaries whilst online

www.cyberchoices.uk



CYBER CHOICES



The Computer Misuse Act 1990

Section 1

Unauthorised access to computer material.

- You watch your friend enter their username and password. You remember their login details and without their permission, later login 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 into 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.



Introduction

Our children are immersed in communications and computing technology, including phones, tablets, laptops, PCs, game consoles, TVs, smart devices and of course the internet.

Many young people are curious and want to explore how these things work, how they interact with each other and what vulnerabilities they have. This can include learning to code and experimenting with tools and techniques discovered online, on video streaming websites, or discussed in forums.

These are great skills to have and the cyber security industry is desperately short of people with them. This means that salaries and prospects in that sector are lucrative. However some people make poor choices and use such skills illegally, often in ignorance of the law. The average age of someone convicted of cyber crime is much younger than other crime types — offenders are often teenagers.

Some young people are vulnerable to becoming involved in cyber crime or have already committed offences. They may be motivated by a desire to challenge their skills, boredom or a lack of understanding of the law and the consequences of breaking it. They may be illegally hacking or using stressor services while gaming for example. The Cyber Choices team want to prevent this through the education of young people and showing them the legal route.

What is and isn't ok?

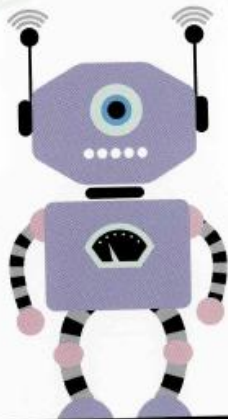
Using the internet, coding and testing skills on legal websites is great. So is playing online games with friends.

Enjoy exploring websites like those on page 6 and finding your own too but, make sure you do not break the law when practicing.

To avoid doing something wrong there are four main things to remember:

- Don't access anyone else's computer, device, network or their accounts without their permission
- Don't do anything that stops someone else's computer, network or device working properly, without the owners permission
- Don't change the way a computer, device, network or website works without the owner's permission
- Don't download, make or supply anything for the purpose of committing cyber crime

Ask a trusted adult if you are unsure about what you or others are doing.



What to remember?

Consequences of breaking the Computer Misuse Act 1990 may include:

- Receiving a visit and warning from the police or NCA officers
- Being arrested
- Getting a criminal record
- Having devices seized
- Being banned or limited in your internet use
- Being expelled from school
- Not being able to get the job you want
- Not being able to travel to certain countries
- ... or all of the above!

We hope you found this Cyber Choices information useful. Used correctly, skills in digital technology and computing can lead to an exciting and well-paid job in the future. Companies really want young people who are good at these things.



Choose the legal or illegal path?

Young people with an aptitude for coding or hacking have a life choice. Will your child choose the legal or illegal path?

If your child has an interest in computers/technology, it's important to have a discussion with them about their use of it. Recognising and engaging with this interest is key to ensuring that they follow the correct pathway.



If you're concerned, talk to your child about the importance of honesty and legality. Explain the consequences of involvement in cyber crime and of breaking the Computer Misuse Act 1990, as detailed within this section. Explain the enjoyable, lucrative and legal options available to them. These include coding, engineering, web development, penetration testing, security operations, law enforcement and many more roles in both the public and private sectors.

Search for computing and coding clubs available in your area and encourage your child to join the appropriate one for their age and ability.

Consequences of breaking the Computer Misuse Act 1990 may include:

- Receiving a visit and warning from the police or NCA officers
- Being arrested
- Getting a criminal record
- Having devices seized
- Being banned or limited in your internet use
- Being expelled from school
- Not being able to get the job you want
- Not being able to travel to certain countries

...or all of the above!

Resources

The Cyber Choices website gives more information on cyber crime and preventing young people from committing it...

www.cyberchoices.uk

There are numerous fun, exciting and stimulating online activities available to test, challenge and develop cyber skills, whether or not your child is considering a career in tech.

CODING

If a young person has an interest in coding, there are lots of online resources and clubs where they can progress their abilities.

Codecademy

Filled with online resources where young people can progress their knowledge.

www.codecademy.com

CoderDojo

Free, local coding clubs worldwide for young people.

www.coderdojo.com





Code Club

A global network of free coding clubs for 9–13 year olds, where they can create games, animations and web pages using Scratch, Python or HTML/CSS.

www.codeclub.org/en/

SKILLS CHALLENGE

Online challenge to test and sharpen cyber skills.

Cyber Security Challenge

Competitions designed to test cyber skills, created by industry professionals looking for the next generation of cyber defenders.

www.cybersecuritychallenge.org.uk

GOVERNMENT PROGRAMMES

Initiatives run by the UK government to sharpen cyber skills and find the next generation of cyber talent.

CyberFirst

Developing the UK's next generation of cyber professionals through student bursaries, courses and competitions. For 11–17 year olds.

www.ncsc.gov.uk/cyberfirst/overview

Cyber Explorers

A fun, free interactive learning platform for those aged 11–14. It showcases how skills taught in class are linked to real world situations, through an immersive, gamified learning experience.

www.cyberexplorers.co.uk



Online training

There are online platforms available to sharpen cyber skills.

Hack The Box

A gamified and hands-on training platform that helps young people learn and advance their skills in penetration testing and cyber security.

www.hackthebox.eu

Vulnhub

Provides online materials allowing users to gain practical hands-on experience with digital security, computer applications and network administration tasks.

www.vulnhub.com

Cybrary

Online IT and cyber security training platform. Self-paced learning, ideal for a young person to grow their skill set.

www.cybrary.it

SANS Cyber Aces

An online course that teaches the core concepts needed to assess and protect information security systems.

www.cyberaces.org

Glossary

Anti-Virus

Software that is designed to detect, stop and remove viruses and other kinds of malicious software.

Bitcoin

An electronic currency which can be used to purchase goods or services online.

Black Hat / Illegal

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 or Distributed Denial of Service attack. Also known as a stressor.

Botnet

A botnet is a group of infected computers controlled by a single command. Criminals can create such a network by infecting individuals' computers with malware to gain control of them.

Cloud

Storing and accessing computing and storage over the internet, for example — software, databases and services.

Denial of Service (DoS) and Distributed Denial of Service (DDoS)

A cyber attack involving the bombarding of a website or web service (such as email) by sending it multiple requests / data messages. If these come from multiple origins simultaneously it is 'Distributed'. These usually involve a botnet being used to carry out the attack.



Hacker

Someone with computer skills who uses them to break into computers, systems and networks (legally or not).

Malware

This is an abbreviation of malicious software. A term that includes viruses, trojans, worms, ransomware or any code or content that could have an adverse impact on a device or system.

Phishing

The sending of untargeted, fraudulent messages to many people, usually to infect the recipient's system with malware by encouraging them to visit a fake website or click on a link.

Ransomware

A type of malware that makes data on systems unusable or encrypted until the victim makes a ransom payment in order to decrypt their data — payment is commonly requested in bitcoin.

Remote Access Trojan (RAT)

A hard to detect type of malware that infects a target's system, and allows the infector complete control over that system including to passwords, data and attached microphones/cameras. Also known as, RAT or Remote Access Tool.

Social Engineering

Manipulating people into doing something unwittingly. This includes divulging personal, technical or other valuable information.

Spear Phishing

The sending of targeted fraudulent messages to selected people, usually to infect the recipient's system with malware by encouraging them to visit a fake website or click on a link.

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.

White Hat / Legal

A legal computer hacker, or computer security specialist, who specialises in lawful penetration testing or other security testing.

