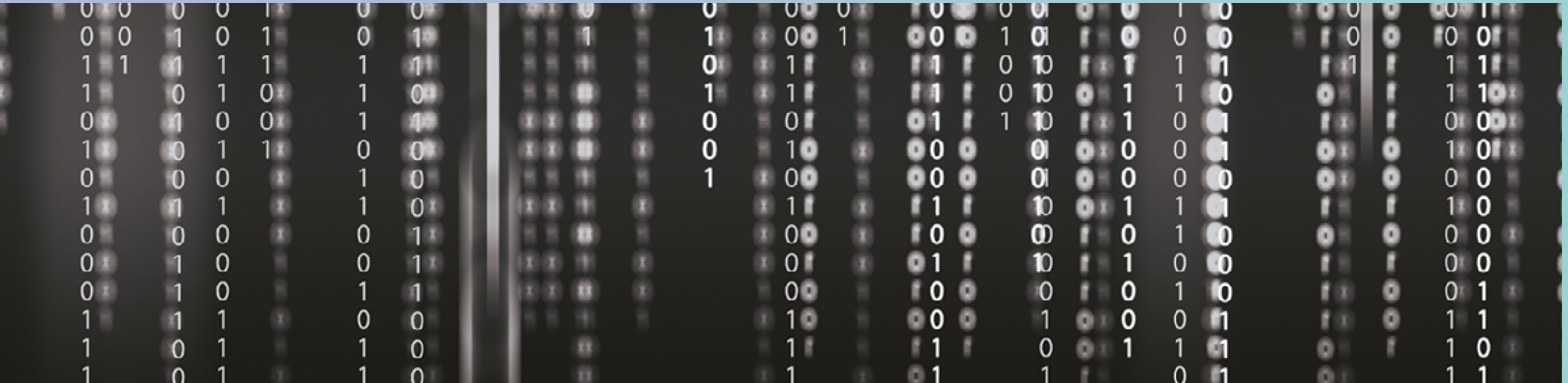
FOR TEACHERS

HACKING IT LEGAL

Helping young people develop **cyber skills**

CYBER CHOICES

Contents



Hello

THANK YOU FOR TAKING THE TIME TO PICK UP THIS BOOKLET

It's been designed to introduce the Cyber Choices programme to teachers and explain how it can help students who may be vulnerable to becoming involved in cyber crime or have begun committing offences.

Introduction

Young people 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.

Cyber Choices

The Cyber Choices network was created to help people make positive choices and use their cyber skills in a legal way.

This is a national programme co-ordinated by the National Crime Agency and delivered by the Regional Cyber Choices Network and Local Police Force Cyber Teams.

The aims of the programme are to:

- Explaining the difference between legal and illegal cyber activity
- Encouraging individuals to make informed choices in their use of technology
- Increasing awareness of the Computer Misuse Act 1990
- Promoting positive, legal cyber opportunities

We achieve these by:

- Engaging with and providing resources to teachers, schools, youth clubs or other organisations
- Attending events such as gaming and computer exhibitions
- Promoting interesting and legal ways to use and develop cyber skills including online competitions

We also work with specific individuals who may be vulnerable to becoming involved in cyber crime or in some cases, have committed offences, to divert them onto a more positive path

Choose the legal or illegal path?

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

If your student 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 student 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, security operations, law enforcement, legal hacking (penetration testing) and many more roles in both the public and private sectors.

Search for computing and coding clubs available in your area and encourage your student 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!

Cyber Choices

Engaging with Cyber Choices

Anyone can contact the Cyber Choices team, including parents, teachers, social workers or law enforcement.

If you're concerned a student or someone you know may be at risk of being involved in cyber crime and would like some advice, you can find our contact details on our **www.cyberchoices.uk** website.

In most cases, the NCA or one of our regional/local partners will provide you with expert advice or can talk to your student before things go too far.

Please note, the Cyber Choices team cannot work with anyone who's subject to a cyber crime investigation until the conclusion of the case. Working with the Cyber Choices team does not prevent an individual being prosecuted for crimes committed, however there may be possibilities for alternative.

Information packs

A range of these information packs are available offering information for various age groups, as well as a leaflet that explains the Computer Misuse Act 1990.

Please visit us on **www.cyberchoices.uk** to find digital copies of these.

The Computer Misuse Act 1990

Section 1	Unauthorised access to computer material.
Section 2	Unauthorised access with intent to commit or facilitate commission of further offences.
Section 3	Unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer.
Section 3ZA	Unauthorised acts causing, or creating risk of, serious damage.
Section 3A	Making, supplying or obtaining articles for use in offence under section 1, 3 or 3ZA.

A criminal record could affect your education and further career prospects so get to know the legal boundaries whilst online.

Read more on page 4

For example

- Adam watches his friend enter their username and password. Adam remembers their login details and without their permission, later logs in and reads all their messages.
- You leave your tablet on the sofa. Without your permission, Raj accesses your gaming account and buys game credits with the attached credit card.
- Sarah is playing an online game with a friend who scores higher than her. Sarah uses a 'Booter' tool knowing it will knock them offline, so she can win the game.
- Kim hacks into a police network. This results in delays to emergency calls and even though it was not her intention, she was reckless in her actions.
- You leave your tablet on the sofa. Without your permission, Raj accesses your gaming account and buys game credits with the attached credit card.

Resources

The National Crime Agency Cyber Choices website gives more information on cyber crime and preventing young people from committing it.
www.cyberchoices.uk

Whether or not a student is considering a career in tech there are numerous fun, exciting and stimulating online activities to legally test, challenge and develop their cyber skills.
We have provided a range of these over the next few pages.

LESSON PLANS

The National Crime Agency have worked with the PSHE association to provide two free Key Stage Three lesson plans on the causes and effects of cyber crime and how to avoid it.
www.pshe-association.org.uk/curriculum-and-resources/resources/exploring-cybercrime-ks3-lesson-plans-national

Create an account with Barefoot to view lesson plans and activities suitable for ages 6 - 7, 7 - 9 and 9 – 11. From online ownership and permissions to the law and password protection – these interactive and engaging resources will keep your pupils more secure by being one step ahead online.
www.barefootcomputing.org/cyber

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 future 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 material 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

Further education

If a young person has an interest in furthering their learning, the following resources provide a wealth of information.

NCSC
The National Cyber Security Centre website contains a lot of information on both academic and professional qualifications in cyber security.
www.ncsc.gov.uk

UCAS
The Universities and Colleges Admissions Service has full details has full details of university courses and entry requirements. The site also details apprenticeships and there are a number of institutions offering cyber security as a specialism.
www.ucas.com

Future careers

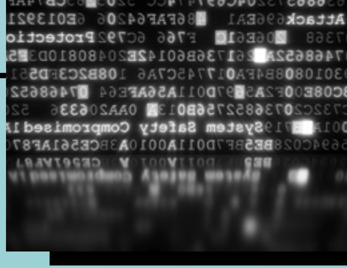
Skills in coding, gaming, computer programming, cyber security or anything tech related are in high demand. There are many careers and opportunities available to someone with an interest in these areas.

TechFuture Careers
A great place to find out about the exciting tech roles available in companies from loads of different sectors. Whether a young person wants to work in fashion, music, media or business, there's a tech role for them.
www.tpdegrees.com/careers

Girl Geeks
Supports untapped talent and females in STEM (Science, Technology, Engineering and Maths) through offering inspiration, connections and opportunities.
www.girlgeeks.uk

Inspired Careers
An innovative virtual hub that explores all of the job roles and career paths open. There are currently 87 different roles listed in cyber security.
www.inspiredcareers.org

CREST
An international not-for-profit accreditation and certification body that represents and supports the technical information security market. CREST has produced some careers guidance for those that are looking to go into cyber security.
www.crest-approved.org/professional-development/crest-careers-guides/index.html



Curious to know how much can be earned working in cyber security?
www.itjobswatch.co.uk/jobs/uk/cybersecurity.do

Traineeships
These are designed to help people who want to get an apprenticeship or job but don't yet have appropriate skills or experience.
www.gov.uk/government/collections/traineeships-programme

Apprenticeships
These are available through college websites and the Government site below.
www.findapprenticeship.service.gov.uk/apprenticeshipsearch

Bug Bounties
Many companies now offer 'bug bounty' schemes. They offer financial incentives for hackers who find and report vulnerabilities in their systems so they can be rectified. These can be a great way for hackers to challenge their skills whilst making money. However, it is essential that the terms and conditions of these schemes are read and strictly adhered to. Failure to follow these or to report vulnerabilities correctly can result in individuals inadvertently committing crime.

All the third party websites listed are publicly available for personal development. They are not necessarily endorsed, supported or monitored by the NCA or UK law enforcement.

All links and web addresses were checked and verified to be correct at the time of publication.

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.

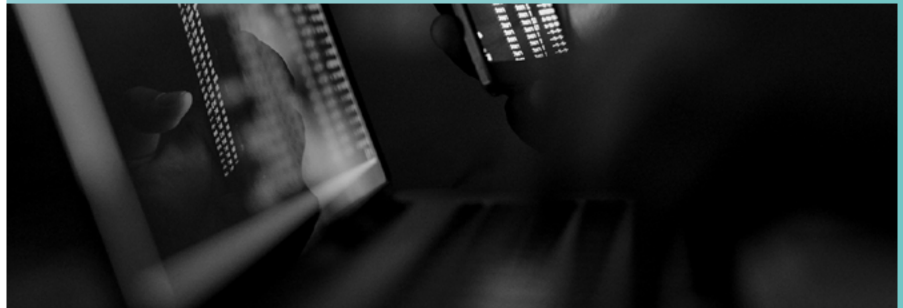
Denial of Service (DoS) and Distributed Denial of Service (DDoS)
A cyber attack involving the bombarding of a website or web service (such as email) by sending it multiple requests / data messages. If these come from multiple origins simultaneously it is 'Distributed'. These usually involve a botnet 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.

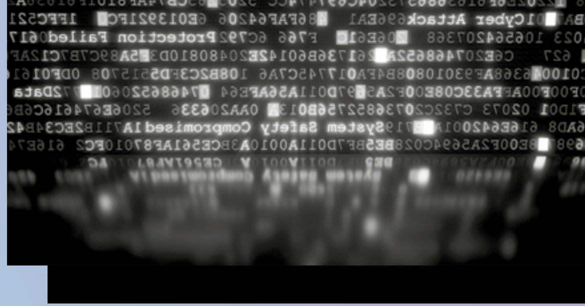
White Hat / Legal
A legal computer hacker, or computer security specialist, who specialises in lawful penetration testing or other security testing.

Get in touch

If you have students that are interested in tech, whether it be coding, exploring the web or gaming, encourage them to build their skills, practice and learn. There are lots of opportunities in cyber. They have a bright future ahead.

Do take the time to have a conversation with students and make sure they understand how to keep it legal and stay safe online. It's important they are aware of the consequences of getting involved in cyber crime. Help them make the right Cyber Choices.

If you would like any further information or advice on Cyber Choices, please visit us at **www.cyberchoices.uk** for more resources and our contact details.



Notes

www.cyberchoices.uk

Helping you choose a positive and legal path