FOR TEACHERS/
SAFEGUARDING
STAFF

HACKING IT LEGAL

Helping young people develop **cyber skills**

CYBER CHOICES

Contents

Hello

THANK YOU FOR TAKING THE TIME TO PICK UP THIS BROCHURE

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:

- Explain the difference between legal and illegal cyber activity
- Encourage individuals to make informed choices in their use of technology
- Increase awareness of the Computer Misuse Act 1990
- Promote 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.

Working with the Cyber Choices team does not prevent an individual being prosecuted for crimes committed, however there may be possibilities for an alternative.

Information packs

A range of 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.

Safeguarding in Schools

Cyber Choices features in the Department for Education's report 'Keeping Children Safe in Education' as well as well as the National Police Chiefs' Council's report 'When to Phone the police'
www.gov.uk/government/publications/keeping-children-safe-in-education--2

www.npcc.police.uk/SysSiteAssets/media/downloads/publications/publications-log/2020/when-to-call-the-police--guidance-for-schools-and-colleges.pdf

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 6

For example

- 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.
- 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.
- 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.
- You hack a phone company. Your hack stops some people phoning the Police when they are in danger. You didn’t mean for this to happen but you were reckless.
- 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.

Resources

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

For more information on what is illegal online activity, debunking the Computer Misuse Act 1990 and how to get in contact with us visit **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 lesson plans on the causes and effects of cyber crime and how to avoid it. Links to view and download these lessons are available through **www.cyberchoices.uk**

CODING

Computer programming or 'Coding' can be described as writing instructions in a programming language that a computer follows to perform specific tasks.

Using coding, individuals can build software, create websites, run applications, design video games and so much more.

There are numerous online resources available to allow anyone with an interest to learn how to code in any number of programming languages, such as Python, Java and HTML.

Resources available through the Cyber Choice's website.

Online training

There are online platforms to sharpen cyber skills.

The online resources available don't just stop at coding there are loads more cyber skills that can be learned through interactive platforms that allow students to practice what they've learned in a safe to fail environment.

Cloud Computing, AI and Machine learning, Networking, Ethical Hacking, Digital Forensics and Scripting are just some of the topics in which students can progress their knowledge and practice their skills.

Some of these skills will become the building blocks for a career in cyber.

Resources available through the Cyber Choice's website **www.cyberchoices.uk**

Online training

GOVERNMENT PROGRAMMES

TechFirst - Tech Youth
Developing the UK's next generation of cyber and tech professionals through student bursaries, courses for 11–18 year olds and competitions.
www.gov.uk/guidance/techfirst

Cyber Explorers
A fun, free interactive learning platform for those aged 11-14 backed by His Majesty's Governments Department for Science, Innovation and Technology (DSIT). It showcases how skills taught in class are linked to real world situations, through an immersive, gamified learning experience.
www.cyberexplorers.co.uk

Further education

If you have an interest in furthering your learning, the following resources provide a wealth of information

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

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/section/education-skills/schools

Future careers

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

There are so many careers in Cyber out there and so much information available online. Why not encourage your students to get searching...“What does a Special Operations Centre Analyst do?” or “What skills do I need to become a Penetration Tester?”

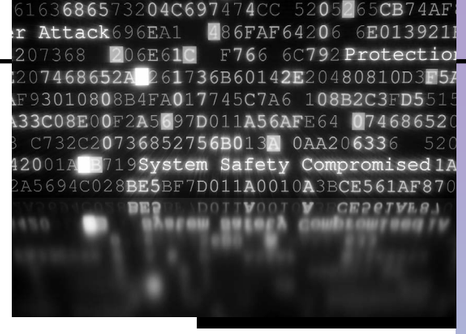
CREST
An international not-for-profit accreditation and certification body that represents and supports the technical information security market.

CREST has produced some careers guidance if your students are looking to go into cyber security.
www.crest-approved.org/skills-certifications-careers/career-path/

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

Careers Service
The National Careers Service provides free and impartial advice, information and guidance on different careers including those in Cyber. The Service is available to anyone aged 13+ no matter what stage of the careers journey you’re at.
nationalcareers.service.gov.uk/explore-careers

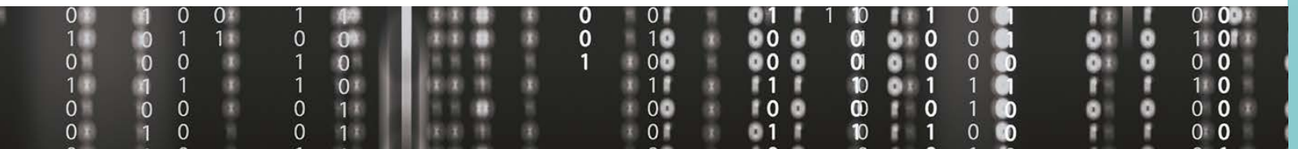
Bug Bounties
Many companies now offer ‘bug bounty’ schemes. They offer financial incentives for hackers who find and report vulnerabilities in their systems so they can be rectified. These can be a great way for hackers to challenge their skills whilst making money. However, it is essential that the 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.



Esports

Esports (electronic sports) is competitive video gaming where players play against each other in teams. Like with any other sport there are opportunities for individuals to learn and develop their core sports skills but also discipline, critical thinking, team working and communication skills.

There is often a crossover between those with an interest in cyber and those with an interest in video gaming and therefore esports offer a unique opportunity to divert potential cyber offenders towards a better pathway through which they can utilise some of their cyber skills.



British Esports

Established with a vision to promote and nurture future esports talent and shape the landscape of competitive gaming throughout the UK and internationally through developing grassroots esports, cutting edge curriculum and career pathways.

There are opportunities for individuals to represent their school, college or university through the British Esports Student Champs (age 12-19) or at University through National Student Esports and to study esports qualifications such as the Esports Leadership Programme, engage with Esports as part of the Duke of Edinburgh Award or study esports full time in further and higher education through the Level 2 to Level 5 National and Higher National Qualifications in esports that support progression into a wide range of future careers.

You can learn more by visiting the British Esports website **britishesports.org/esports-and-education/**

With 9 in 10 young people already playing video games, Teachers and Safeguarding Staff have a responsibility and duty to care towards young people. ‘Duty to Care in Esports’ is a free, certified, learning programme which prioritises positive coaching and engagement with players and teams by focusing on seven key pillars of knowledge and understanding which includes a Cyber Choices module. **britishesports.org/esports-and-education/esports-courses/duty-to-care-in-esports/**

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.

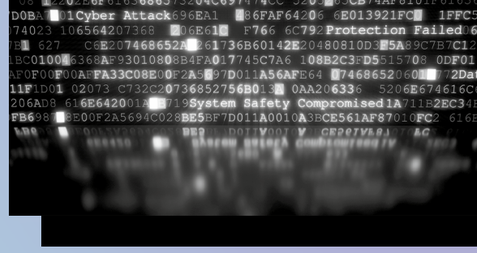
Remote Access Trojan (RAT)
A hard to detect type of malware that infects a target's system, and allows the infector complete control over that system including to passwords, data and attached microphones/cameras. Also known as, RAT or Remote Access Tool.

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