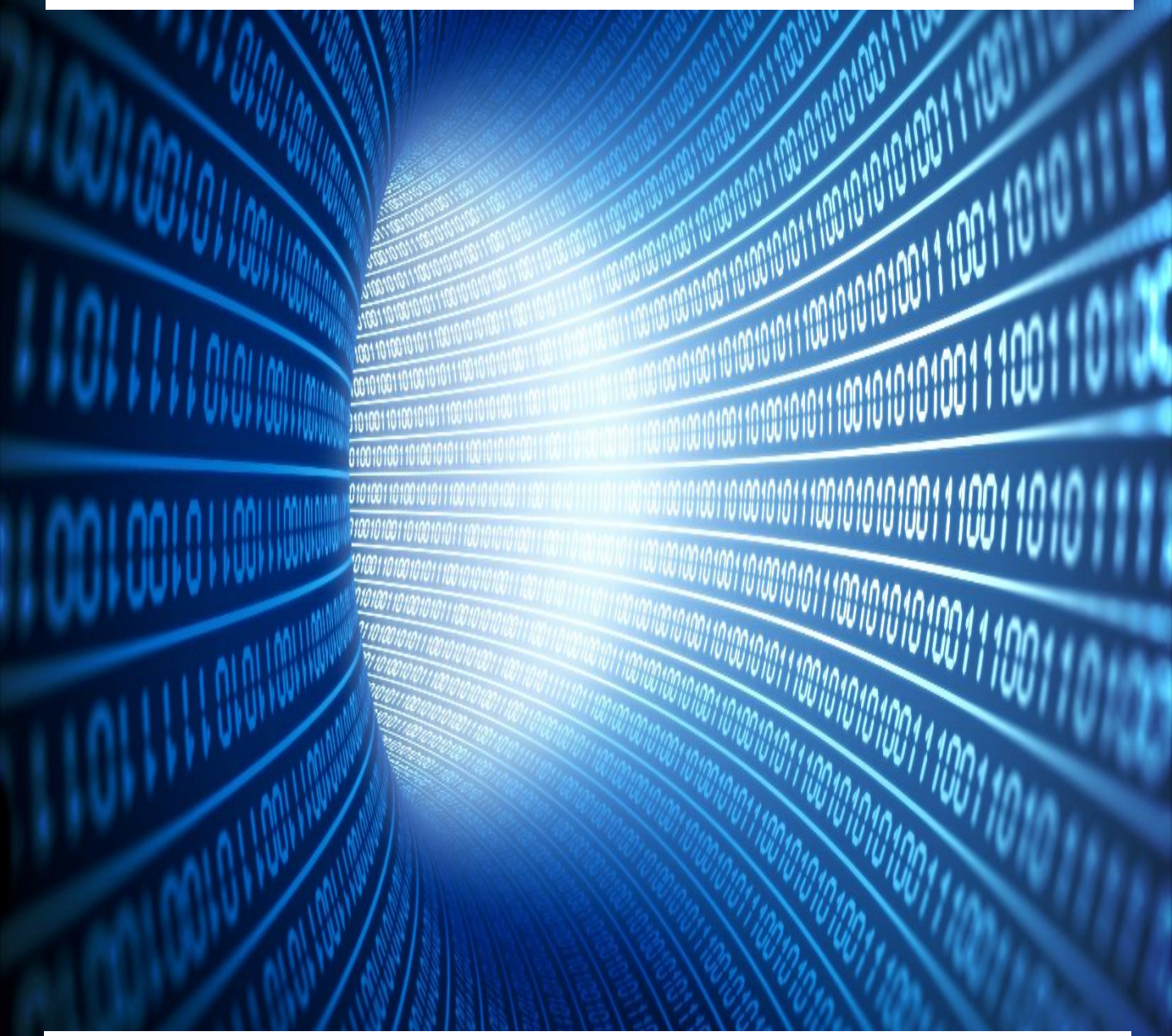
YH ROCU

Yorkshire & Humber
REGIONAL CYBER CRIME UNIT



CYBER PREVENT / PROTECT

PARENTS GUIDE

Yhrocu.org.uk @YH_CyberProtect YorkshireandHumberRCCU

CYBER CRIME MATTERS
PREVENTION IS KEY

The average age of someone arrested for a cybercrime is just 17 years old

– BUT –

There is a predicted 1.8 million shortfall in cyber security professionals by 2022

This booklet is aimed at increasing your knowledge of both the negatives and the positives of the cyber world. It will highlight and describe criminal offences online, opportunities within the information technology industry and help you keep safe whilst online. Our aim is to support and protect people so they can make the right decisions in life.

Now is the ideal time for anyone looking for a career within the Information Technology industry. There's hundreds of different roles to suit every type of interest. Best of all, not every role requires significant technical skills, some roles for example may be suited to problem solvers and strategic thinkers.

The most important aspect is that people understand what is and isn't legal, so the right choices can be made (intentional or otherwise).

Any questions or if further advice is needed please contact us at:
cyber@yhrocu.pnn.police.uk

YH ROCU Yorkshire & Humber REGIONAL CYBER CRIME UNIT

The National Crime Agency coordinate the national Cyber Prevent Strategy with the 10 Regional Organised Crime Units - including us, YHROCU – delivering the project.

Cyber Prevent Objectives:

- To deter individuals from getting involved in cyber crime.
- To prevent individuals from moving deeper into cyber crime.
- To prevent individuals from re-offending.

Prevent Key Messages:

- Increase knowledge of the Computer Misuse Act 1990.
- Increase knowledge of consequences due to involvement in cyber crime, including the growth of law enforcement capabilities.
- Promotion of positive opportunities to develop and use cyber skills legally.

Prevent Target Audiences:

- Identify emerging UK individuals on the cusp or in early stages of involvement in cyber crime.
- Identify low level customers or facilitators of cyber crime i.e. users of 'off the shelf' tools such as stressors.
- Identify cyber offenders who have received a caution or conviction.
- Support and enlighten parents, teachers, carers, youth workers and others likely to be in contact with cyber active young people.

Are you interested in helping fight Cyber Crime?

The NCA run a Cyber Specials programme where you can volunteer your time fighting cyber criminals. This will also enhance your reputation and credentials.
www.nationalcrimeagency.gov.uk/careers/specials

YH ROCU Yorkshire & Humber REGIONAL CYBER CRIME UNIT

The Computer Misuse Act 1990, makes the following actions illegal:

Offence	Example of potential unlawful activity
Section 1 > Unauthorised access to computer material	Without them knowing, you watched your friend put their password into their phone. You then used it to gain access to their phone and download their photos
Section 2 > Unauthorised access with intent to commit or facilitate commission of further offences	Without their permission, you accessed your friend's smartphone, obtaining their bank details, so you could transfer money from their account
Section 3 > Unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer	You used a booter tool to knock a friend offline from an online game
Section 3ZA > Unauthorised acts causing, or creating risk of, serious damage	You hacked into the computer system of a Government Agency and were reckless as to the consequences. National security was undermined
Section 3A > Making, supplying or obtaining articles for use in another CMA offence	You downloaded a product to deploy malware to a friend's computer, so you could control it. You didn't even get the chance to use it

Yorkshire & Humber
REGIONAL CYBER CRIME UNIT
YH ROCU

UK Law Enforcement

UK Law Enforcement will deal with cyber offenders in a robust and dynamic manner.
If you are offending, expect a visit from our colleagues very early one morning. All computer devices and all digital storage will be seized for interrogation. You are likely to be arrested and kept in a cell, alone, awaiting interview.

If you are assessed as being on the cusp of cyber offending, you may be given a Cease and Desist Notice. This is a warning that your cyber activity is known to Law Enforcement and a failure to stop offending may lead to an early morning visit.

A Cease and Desist Notice would also be used in any future prosecution against you as evidence of your unwillingness to respond positively to this warning.

Yorkshire & Humber
YH ROCU REGIONAL CYBER CRIME UNIT

Consequences of Conviction

If you are dealt with for a Computer Misuse Act offence you may receive:

- A caution – with or without conditions you must abide by
- A prison sentence
- An unlimited fine
- A Serious Crime Prevention Order *or* Criminal Behaviour Order – restrictions may include prohibitions on your use of the internet, having Police monitoring software on your devices and cooperating with the Police Cyber Prevent team.

Other things to think about…

A conviction for a cyber offence may well impact upon your ability to apply for many employment opportunities. There are a number of companies that will not employ anyone with a criminal conviction, and you have to declare your conviction for a set period of time under the Rehabilitation of Offenders Act.

A criminal record may be publically reported – these reports will exist online for a long time. Many employers now use research companies to find out everything they can about you including those on public reports.

Being arrested – not even convicted – for an offence will have an impact upon your ability to visit certain foreign countries. For example, an arrest will mean that visa free entry into the USA will no longer be available to you. Australia may also refuse a visa.

A conviction is likely to impact upon your ability to obtain credit, including a student loan or a mortgage. Insurance on cars and homes is likely to be more expensive.

A conviction may affect your ability to rent property – if you are in social housing it could jeopardise your tenancy.

YH ROCU Yorkshire & Humber REGIONAL CYBER CRIME UNIT

Spotting The Signs

Research suggests that individuals can now be addicted to technology and to the internet. Such fascination or obsession could identify those already committing, or at risk of committing cybercrime and in many situations unwittingly or unknowingly commit an offence.

Here are some further indicators (Please note these are merely indicators!)

Physical Signs

- Backache
- Headaches
- Weight gain or loss
- Disturbances in sleep
- Carpal tunnel syndrome
- Blurred or strained vision

Emotional Signs

- Feelings of guilt
- Anxiety
- Depression
- Dishonesty
- Euphoric feelings when in front of the computer
- Unable to keep schedules
- No sense of time
- Isolation
- Defensiveness
- Work avoidance
- Agitation

Further Examples

- Spending a long time in front of a computer for reasons that are not work-related

- Irritability or bad tempered if access to the internet is blocked or restricted

- Pleasurable anticipation of internet use is common, although many internet addicts see their internet overuse as a form of stress management

- Multiplayer role-play gamers may also see their usage as a form of social contact

- As the addiction becomes more severe, internet usage becomes more important than most other activities and social interactions reduce.

YH ROCU Yorkshire & Humber REGIONAL CYBER CRIME UNIT

Careers in Cyber Security

The world is in need of cyber security professionals. With a predicted worldwide shortfall of 1.8 million by 2022, now is the perfect time to get into the industry. There are lots of different roles in cyber security, each with a different specialism and emphasising on technical or strategic skills.

Penetration Tester / Certified Ethical Hacker

A penetration tester or ethical hacker tries to find and exploit security vulnerabilities in web-based systems or applications, networks or other computer based systems. This is legal hacking in accordance with a set of ethical and moral rules, and in accordance with guidance from your employer and the client paying for it. The aim is to improve organisational security. www.eccouncil.org/

Security Analyst or Engineer

A security analyst detects and prevents cyber threats to organisations; planning and implementing methods of protecting networks. An engineer designs, builds and maintains IT security systems. They work out of the Security Operations Centre.

Security Incident Responder

The incident responder is the person who reacts to threats and tries to defeat them. They use system and network monitoring tools to keep one step ahead of the threats, and forensic analysis tools to digest the threats, minimise damage and mitigate the future risk.

Information Assurance Analyst

These analysts are responsible for designing, planning and deploying changes to the software architecture while maintaining the integrity of the data held and the functionality the business requires. They ensure nobody can access the data improperly.

Certified Information Systems Security Professional (CISSP)

CISSP is a qualification which demonstrates excellence and experience (minimum 5 years) in information security and is generally for those in a more senior role managing a cyber security team. www.isc2.org/Certifications/CISSP

YH ROCU Yorkshire & Humber REGIONAL CYBER CRIME UNIT

How to get into a Cyber Career

There are several routes into a cyber career no matter which role you have chosen.

Degree or Degree Apprenticeship

A degree is the typical route to a career. Degree apprenticeships are now an option which combine learning and practical work with an employer, and you can get paid. The typical qualification is a computer science degree, but there are now also specialist cyber security degrees offered by some universities that have diversified. Entry requirements vary considerably but Further Education qualifications such as A levels (or equivalent) are required. Full details on courses, entry requirements and degree apprenticeships are available from UCAS: www.ucas.com/

There is some useful information available:
www.thetechpartnership.com/techfuture/techfuture-careers/

Really talented? Look on www.gchq-careers.co.uk/early-careers/apprenticeships.html

Apprenticeship

An apprenticeship is a more hands on way of learning and becoming qualified. You'll spend some time in college but also lots of time working with mentors teaching in a hands-on manner. There are different tiers of apprenticeship depending on your starting point. The bonus is that you will earn a wage and get holiday pay. Some employers may hire you on completion of an apprenticeship. Search at: www.gov.uk/apply-apprenticeship

Or Google 'Cyber Apprenticeship'

Self-Qualification

The cyber security industry does not just rely on traditional qualifications and, indeed, even if you have a degree there is a need for ongoing continuous professional development. There are qualifications such as CISSP and CEH which can support this. Fast-track courses are available and you can earn you these qualifications in a week or two. They're not cheap, but you'll quickly recoup the cost. Research what qualifications are required for the role you are interested in, and then explore online courses as well as residential fast track courses from reputable providers. The CREST website can identify these providers. www.crest-approved.org/

Getting Experience

To get into the world of cyber security you will likely need some kind of qualification (industry and/or academic) and some form of experience. Getting experience can be daunting but there are lots of ways to boost your CV.

Volunteering

Volunteering can be a good place to get some skills and experience which an employer would desire. There are lots of Code Clubs and Coder Dojos around the country who seek cyber talented individuals to support them. Employers see that you are 'giving something back' and this is a desirable trait. It can improve your skills around teaching as well as social skills. You could push yourself to present to audiences. Helping run the club can demonstrate administrative skills.
coderdojo.com/ (7 to 17 year olds)
www.codeclub.org.uk/ (9 to 13 year olds)

Work Experience

Work experience is often viewed as something only people of school age do, which is often arranged for them. Anyone can ask for unpaid work experience. Not all companies are geared up to offer it, and not everyone can deal with the *risk management* involved in allowing access to systems. "Don't ask, don't get" is true. Be bold – identify a company you might want to work for and make contact. They may even take you on and pay for your education:
www.prospects.ac.uk/jobs-and-work-experience/work-experience-and-internships in particular the section on how to ask for work experience.

Going it Alone

Once you've developed some skills do some independent work. When you're starting out, if you can demonstrate *case studies* on work you have done an employer is more likely to pay attention to you. Learn how to write a formal security report. Consider bug bounty work – but make sure you're doing it ethically and following responsible disclosure guidelines. Write about your successes. Then when you get an interview you can talk in detail about what you did. Append a case study to your CV.

What is responsible disclosure: en.wikipedia.org/wiki/Responsible_disclosure
Responsible disclosure platform for bug bounty hunters: www.hackerone.com/

Do you know something about cyber criminals?
Do the right thing… Tell Us!

The UK Government's National Security Strategy has recognised the cyber threat as one of four 'Tier One' risks to the UK's security, sitting alongside international terrorism. The cost of cyber-crime to the UK is estimated to be £27 billion each year.

There are plenty of ways in which cyber dependant crimes are discussed, organised and committed. Cyber crime is not victimless. Many individuals, small and medium businesses are the victim of this criminal behaviour. The impact is often personally and financially catastrophic. More than 50% of small businesses close down within 6 months of a cyber-attack – impacting on communities and the local economy.

Those individuals within the cyber community who enjoy the more niche areas and have a strong and ethical moral intent should consider helping law enforcement. This could be by providing information about those who may be using their skills or knowledge to hurt others

If you know something that we should know, then please make contact:

Email us at:
Cyber@yhrocu.pnn.police.uk

YH ROCU Yorkshire & Humber REGIONAL CYBER CRIME UNIT

Anonymously via CrimeStoppers:
Crimestoppers-uk.org/

CrimeStoppers. Speak up. Stay safe.

Anonymously via Fearless:
www.Fearless.org/en

fearless.org

YH ROCU Yorkshire & Humber REGIONAL CYBER CRIME UNIT

Are you concerned about someone's online activity. We can help.

If you are worried about what someone is doing online we can help. Now is the time to try and educate them to use their skills in a positive way and avoid criminal sanction. We have included a cyber glossary so that we can provide you with a better understanding.

As the Police we have a legal duty however, the Cyber Prevent aim is to try and divert people positively, not to criminalise unnecessarily.
We can discuss your concerns and worries and signpost you towards resources to help. Please email us at **Cyber@yhrocu.pnn.police.uk.**

We will need your name and contact number. If you could give reasons why you are concerned or information regarding your reasons for contacting us. In the meantime:

- Make sure you know what they are doing online? Who they are communicating with? Can their 'friends' be verified?
- Talk to your child – try to learn about computing with them. You may get a better understanding of what they are doing and what their ability and risk's may be
- Net Aware (www.net-aware.org.uk) will help you understand some of the sites, games or apps they spend time on
- Moderate the amount of time they spend online. More than 4 hours online is deemed excessive, so encourage other non-computer based activities. Your home broadband can restrict these hours automatically, minimising conflict.
- Monitor what they are doing on the computer by placing all devices they have access to in a communal area of the house.

Our remit is ***cyber dependent* crime** – this is crime where the use of information technology is key to the crime such as hacking, computer intrusion or denial of service attacks. Should you have concerns about *cyber enabled* crime such as sexting, questionable images or cyber bullying help is available via the useful links in Appendix C or from your local Police force.

YH ROCU Yorkshire & Humber REGIONAL CYBER CRIME UNIT

Tips to stay safe online

Don't connect to unknown Wi-Fi Hotspots:

When using public Wi-Fi hotspots (for example in a hotel or coffee shop) there is no way to easily find out who controls the hotspot or that it is secure. If you connect to these hotspots, somebody could access:

- Your files (Documents, pictures or anything you display on screen)

- Your login details e.g. username and password of any services/application you use.

The best way to stay safe is to not connect to Wi-Fi hotspots, and instead use your mobile 3G or 4G mobile network where possible. This means you can also use 'tethering' (where your other devices such as laptops share your 3G/4G connection) or a wireless internet 'dongle'. You can also use Virtual Private Networks (VPNs) which encrypt your data before it is sent across the Internet. If you're using third party VPNs, you'll need the technical ability to configure it yourself, and should only use VPNs provided by reputable service providers.

Your Online Identity:

Check your privacy settings on social media accounts and think carefully about what personal information you put online.

- Regularly check your privacy settings. Often software or application updates can restore your settings back to default.

- Think carefully about what information you would want people to know. For example, you could make a custom group so information is only sent to your closest friends and family.

- Avoid sharing sensitive personally identifiable information (PII) such as your date of birth, home address, employment details, financial information etc.

- Check your location services – Your device may track your locations by default so consider checking your settings.

Tips to stay safe online

Passwords:

By using passwords you can help to protect your data. Your laptops, computers, tablets and mobile phones will contain a lot of your own business-critical data, the personal information of your customers, and also details of the online accounts that you access. It is essential that this data is available to you but not available to unauthorised users.

- **Tip 1:** Make sure you switch on password protection. You can set a lock screen password, PIN, or other authentication methods such as fingerprint or face identification. You may still be required to have two methods as a back-up if your fingerprint or face is not recognised.

- **Tip 2:** Use two factor authentication (2FA) for your accounts. If you're given the option to use 2FA for any of your accounts we advise that you setup this additional security feature. 2FA requires two different methods to prove your identity before you can use a service which generally includes password plus one other method. For example a code that's sent to an authenticator application on your mobile phone that you must enter in addition to your password.

- **Tip 3:** Avoid using easy and predictable passwords. You should avoid using any personally identifiable information (PII) which related to you e.g. your surname, middle name, year of birth etc.

The National Cyber Security Centre's advice is to choose
THREE RANDOM WORDS.

(By following this guidance you could then add numbers, special characters, uppercase or lowercase depending on how complex and secure your would like your password to be).

YH ROCU Yorkshire & Humber REGIONAL CYBER CRIME UNIT

Tips to stay safe online

Backups:

We suggest to have back- ups of your data. Think about how much you rely on your data? Now imagine how long you would be able to operate without it. Furthermore, if you have backups of your data that you can quickly recover, you are safer if you suffer from a ransomware attack.

- **Tip 1:** Identify what data you need to back up. Your first step is to identify your essential data or the information that you would need to function. Normally this will comprise of documents, photos, emails, contacts and calendars, most of which are kept in just the common folders on your computer, phone, tablet or network.

- **Tip 2:** Keep your back-up separate from your computer. This may be on a USB stick, on a separate hard-drive or another computer. The access to your backups should be restricted so that they are not accessible by unauthorised users and are not permanently connected (either physically or over a local network) to the device holding the original copy. Furthermore, ransomware (and other malware) can often move to attached storage or back-up to your cloud storage meaning the backup could also be infected. For more resilience, you should consider storing your backups in a different location, so fire or theft won't result in you losing both copies.

- **Tip 3:** Consider using cloud storage. Using cloud storage (where a service provider stores your data on their infrastructure) means your data is physically separate from your location. Your data will be readily available to use and automatic backups can be set for every time a document is edited. Most providers offer a limited amount of storage space for free and further storage at small cost annually or monthly.

YH ROCU Yorkshire & Humber REGIONAL CYBER CRIME UNIT

Tips to stay safe online

Phishing Attacks:

In a phishing attack the attacker sends a fake email purporting to be someone from a reputable organisation and asking for your personal and sensitive information (such as bank details), or containing links e.g. to legitimate websites for harvesting credentials or ransomware.

They may try and trick you into sending money, harvest your details to sell on the dark web or they may have political or ideological motives for accessing your organisation's information. Phishing emails are getting harder to spot, and some will still get past even the most observant users.

- **Tip 1:** Don’t open any emails from people you weren't expecting or do not know.
- **Tip 2:** Never click on links if you are not 100% sure that they are legitimate.
- **Tip 3:** The attacker may personally research you online (known as social engineering) in order to send you emails that look genuine. Be careful what you post, where you’re posting it and who can see it because this information may be gathered and used to make you think the email is legitimate.
- **Tip 4:** Check for errors such as poor spelling and grammar or low quality versions of recognisable logos.
- **Tip 5:** Check the sender’s email address matches the actual company or person it’s trying to represent. Check the full email address in the sender’s section.
- Tip 6: Consider whether you have an account with the sender. If the email stated ‘Click here to view your latest bank statement’ should you click the link if you don’t even have a bank account with that company?

YH ROCU Yorkshire & Humber REGIONAL CYBER CRIME UNIT

Online Resources for Self-Development

There are free resources available which you can use to test and enhance your skills. This may be for your self development, interest or for a chosen career path.

Cyber Security Challenge UK

Online competitions designed to test your cyber security skills. Free to participate, any age. Progress well and you might be invited to participate in the live finals where sponsor companies often cherry pick contestants for jobs. www.cybersecuritychallenge.org.uk/

Digital Cyber Academy- *Available free to anyone with academic .ac.uk email address*

A set of browser based learning labs including challenges. Learn for yourself how to complete the lab, with some guidance. Includes a job portal where the only application requirement is to complete labs chosen by the employer. www.digitalcyberacademy.com/

Futurelearn

Free online learning courses provided by academic providers worldwide – managed by the Open University. *Introduction to Cyber Security* gives a good foundation knowledge. www.futurelearn.com/

EdX

Free online learning courses provided by academic providers worldwide. *CS50* is a good introductory computer science course whereas *CYB001X* a good cyber security introduction. www.edx.org/

Hack the Box

Online platform to test advance penetration testing and cyber security skills. You'll need some skills to get past the invite challenge and through to the main event! www.hackthebox.eu/

Cybrary

An open source cyber security and IT learning platform. Free courses which may prepare you for industry exams should you choose. Paid for by adverts and referral fees when people sign up for exam tracks. www.cybrary.it/

W3 Schools

Large collection of online learning around coding including web and database skills. www.w3schools.com/

Code Academy

Large collection of online learning around coding. www.codecademy.com/

Solo Learn

Large collection of online learning around coding. www.sololearn.com/

Useful Resources

Online safety for under 18s, parents and schools:

Get Safe Online	www.getsafeonline.org
Think U Know – Age specific advice	www.thinkuknow.co.uk
Net Aware - App, game and advice	www.net-aware.org.uk
UK Safer Internet Centre	www.saferinternet.org.uk
Internet Matters – parental advice	www.internetmatters.org
NSPCC	www.nspcc.org.uk
CEOP – reporting and advice	www.ceop.police.uk

Useful Sites for Security:

Have I Been Pwned	www.haveibeenpwned.com
National Cyber Security Centre (Small business infographics)	www.ncsc.gov.uk

Useful Apps:

YOTI – helps children take down images they may have shared
Fing - shows you the devices connected to your Wi-Fi

YouTube Channels:

CEOP :
www.youtube.com/user/ceop
Yorkshire and the Humber ROCU:
www.youtube.com/channel/UC_Ea_aVrfZ_s7XAqMWZbwpg
National Crime Agency:
www.youtube.com/user/NationalCrimeAgency

Check for latest frauds and scams:

Action Fraud	www.actionfraud.police.uk
Take Five	www.takefive-stopfraud.org.uk

Physical Activities:

CoderDojo (7 – 17 yrs old)	coderdojo.com
CodeClub UK (9 – 13 yrs old)	www.codeclub.org.uk
National Citizen Service (15 – 17 yrs old)	www.ncsyes.co.uk

YH ROCU Yorkshire & Humber REGIONAL CYBER CRIME UNIT

Glossary

Antivirus	**Software that is designed to detect, stop and remove viruses and other kinds of malicious software**
App	Short for Application, typically refers to a software program for a smartphone or tablet
Attack (Cyber Attack)	Malicious attempts to damage, disrupt or gain unauthorised access to computer systems, networks or devices, via cyber means
Bitcoin	One of the most popular forms of Cryptocurrency
Black Hat (Hacker)	A malicious hacker – often one who does so purely for the challenge rather than any gain
Booter	Used to implement a DoS or DDoS attack. Also known as a stresser
Botnet	A network of infected devices, connected to the Internet, used to commit coordinated cyber-attacks without their owner's knowledge
Browser	A software application which presents information and services from the Web
Brute Force Attack	Using computational power to automatically enter a huge number of combination of values, usually in order to discover passwords and gain access
Certificate	A form of digital identity for a computer, user of organisation to allow the authentication and secure exchange of information

YH ROCU Yorkshire & Humber REGIONAL CYBER CRIME UNIT

Glossary

Certified Ethical Hacker (CEH)	**A skilled professional who looks for weaknesses and vulnerabilities in target systems using the same knowledge and tools as a malicious hacker, but in a lawful and legitimate way**
Cloud	Where shared computer and storage resources are accessed as an online service instead of hosted locally.
Cryptocurrency	A digital asset in which encryption techniques are used to regulate the generation of units of 'currency' and verify the transfer of funds, operating independently of a central bank
Cyber Security	The protection of devices, services and networks and the information on them from theft or damage
Dictionary Attack	A type of brute force attack in which the attacker uses known dictionary words, phrases or common passwords as their guesses
Denial of Service (DoS) **Distributed DoS (DDoS)**	An attack involving the overloading of a website or web service (such as email) by bombarding it with multiple requests / data messages. If request's come from multiple origins simultaneously it is Distributed. Usually involves a botnet to carry out the attack. Stresser or booter software or websites may be used
Encryption	A mathematical function that protects information by making it unreadable by everyone except those with the key to decode it.
Exploit	May refer to software or data that takes advantage of a vulnerability in a system to cause unintended consequences

YH ROCU Yorkshire & Humber REGIONAL CYBER CRIME UNIT

Glossary

Firewall	**Hardware or software which uses a defined rule set to constrain network traffic to prevent unauthorised access to or from a network**
Grey Hat	(Hacker) A computer hacker who may sometimes violate laws or typical ethical standards, but does not have the malicious intent typical of a black hat hacker and often does legitimate work
Hacker	Someone with computer skills who uses them to break into computers, systems and networks (legitimately or not)
Honeypot **Honeynet**	Decoy system or network to attract potential attackers that helps limit access to actual systems by detecting and deflecting or learning from an attack. Multiple honeypots form a honeynet
Kali	(Linux) A type of Linux operating system which is preconfigured with computer security tools. A favourite with Black Hat hackers too.
Keylogger	Malware that once installed records all keystrokes from a keyboard and then send them back to the Cyber Attacker. Often reveals usernames, passwords, banking details
Linux	A free computer operating system, which can run on the same hardware as Microsoft Windows. Often used to run servers which run the internet and intranets.
Macro	A small program that can automate tasks in applications (such as Microsoft Office) which attackers can exploit to gain access to (or harm) a system.

YH ROCU Yorkshire & Humber REGIONAL CYBER CRIME UNIT

Glossary

Malware	**Malicious software - a term that includes viruses, trojans, worms or any code or content that could have an adverse impact on organisations or individuals**
Network	Two or more computers linked in order to share resources
Penetration Testing **Pentest / Pentester**	Short for penetration test. An authorised test of a computer network or system by a Pentester designed to look for security weaknesses so that they can be fixed
Pharming	An attack on network infrastructure that results in a user being redirected to an illegitimate website despite the user having entered the correct address
Phishing	Untargeted, mass emails sent to many people asking for sensitive information (such as bank details) or encouraging them to visit a fake website. May result in the installation of Malware.
Ransomware	Malicious software that makes data or systems unusable until the Victim makes a payment, usually in Bitcoin
Router	The network device which allows multiple internet enabled devices to connect to other networks, usually over the internet
Smishing	Phishing via SMS: mass text messages sent to users asking for sensitive information (e.g. bank details) or encouraging them to visit a fake website
Social Engineering	Manipulating people into carrying divulging personal or technical information, or carrying out actions such as changing an email address, which is of use to a Cyber Attacker

YH ROCU Yorkshire & Humber REGIONAL CYBER CRIME UNIT

Glossary

Spear Phishing	**A more targeted form of phishing, where the email is designed to look like it's from a person the recipient knows and/or trusts – such as someone in Management or from a finance department.**
Stresser / Stressor	Used to implement a DoS or DDoS attack. Also known as a booter
Trojan	A type of malware or virus disguised as legitimate software. Often used to take remote control of a computer, or extract and send out confidential data
Virus	Programs which can self-replicate and are designed to infect legitimate software programs or systems. May be purely destructive or have other aims. A form of malware
Virtual Private Network (VPN)	Software which creates an encrypted network to allow secure connections for remote users, e.g. in an organisation with offices in multiple locations or allows home working
Vulnerability	A weakness, or flaw, in software, a system or process. An attacker may seek to exploit a vulnerability to gain unauthorised access to a system
Water Holing **Watering Hole Attack**	Setting up a fake website (or compromising a real one) in order to exploit visiting users
Whaling	Highly targeted phishing attacks (masquerading as a legitimate emails) that are aimed at senior executives (Hacker) An ethical computer hacker, or computer security specialist, who specialises in penetration testing or other security testing

YH ROCU Yorkshire & Humber REGIONAL CYBER CRIME UNIT

Glossary

White Hat	**(Hacker) An ethical computer hacker, or computer security specialist, who specialises in penetration testing or other security testing**
Worm	A self-replicating, self-spreading and self-contained program that spreads across a network
Zero Day / 0Day	Recently discovered vulnerabilities (or bugs), not yet known to vendors or antivirus companies, that Cyber Attackers can exploit

YH ROCU Yorkshire & Humber REGIONAL CYBER CRIME UNIT

YH ROCU

Yorkshire & Humber
REGIONAL CYBER CRIME UNIT