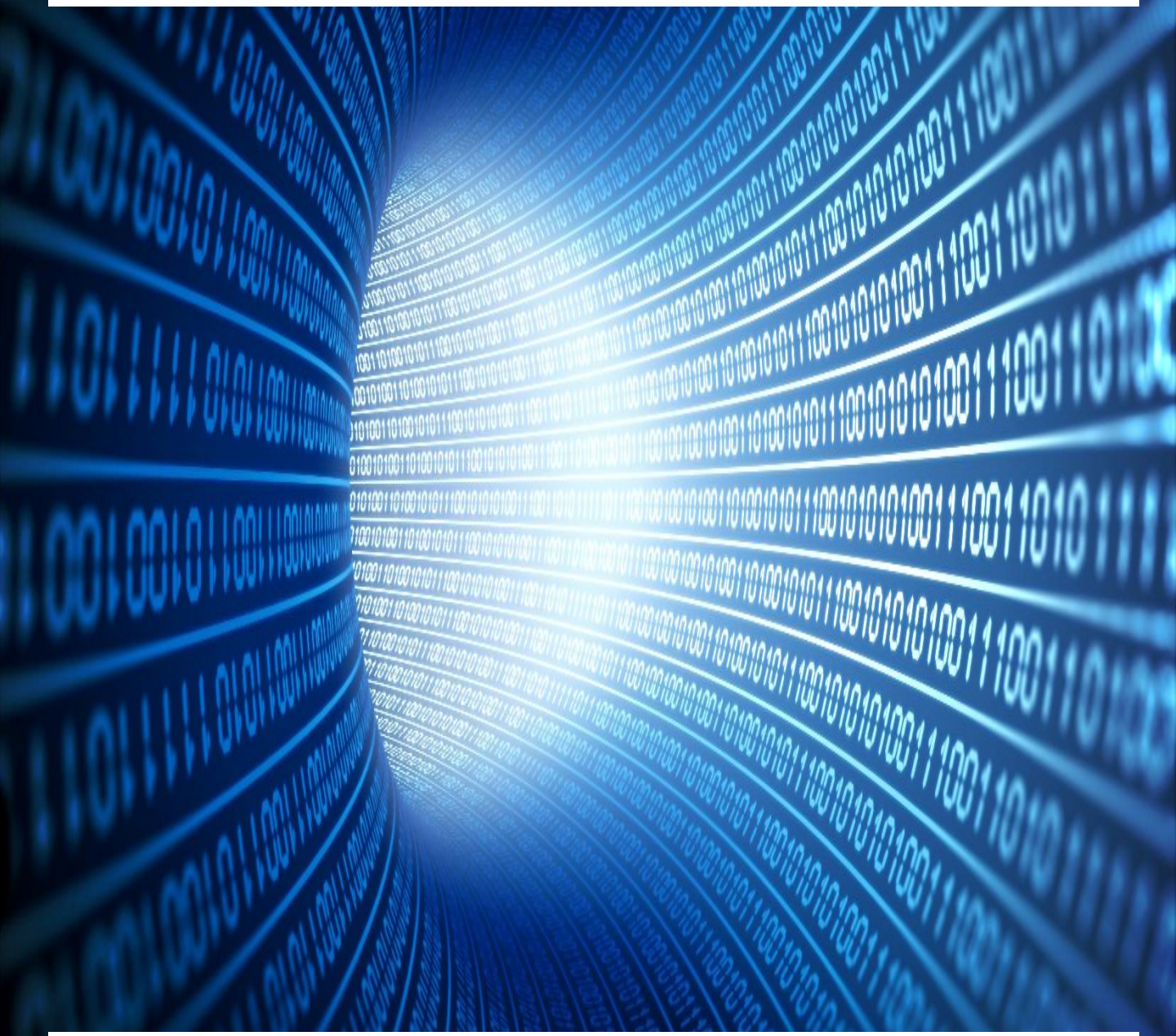
YH ROCU

Yorkshire & Humber
REGIONAL CYBER CRIME UNIT



CYBER PREVENT

EDUCATION PACK

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 the pitfalls and the positives about online activity, what is criminal or not and the opportunities available, in order that you can help support your children to make the right decisions in life.

This is the ideal time for your child to head down the route into employment in a Cyber Security career. There are lots of different roles suiting every different type of interest. Not all require significant technical skill but may be more suited to problem solvers and strategic thinkers.

The most important aspect is that you help them understand what is and isn't legal, so that they don't head down the wrong route to become a Cyber Criminal. As such, we would ask that you sit down and go through the law and consequences with them, before discussing their future career and how to use the resources to develop.

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 cybercrime in the first place.
- 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.

Want to help 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

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

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.

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
- Avoiding doing work
- Agitation

Further Examples

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

- Irritability or bad moods if access to the internet is blocked or has to be abbreviated

- 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 major social problems are likely to follow.

YH ROCU Yorkshire & Humber REGIONAL CYBER CRIME UNIT

Careers in Cyber Security

The world is crying out for 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 emphasis on technical or strategic role – do your own research!

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. https://www.eccouncil.org/

Security Analyst or Engineer
A security analyst detects and prevents cyber threats to organisations, plans and implements 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
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. https://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 good information available:
www.thetechpartnership.com/techfuture/techfuture-careers/

Really talented…
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 will hire you at the conclusion 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. These are qualifications such as CISSP, CEH, etc. There are plenty of fast-track courses which can earn you these in a week or two. They're not cheap, but you'll quickly recoup the cost. Research what qualifications are used for the role you are interested in, and then explore online course offerings as well as residential fast track courses from big name providers. The CREST website can identify these providers. www.crest-approved.org/

YH ROCU Yorkshire & Humber REGIONAL CYBER CRIME UNIT

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. That's on a par with international terrorism. The cost of cyber-crime to the UK is estimated to be £27bn per annum.

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 type of criminal behaviour. The impact is often personally and financially catastrophic. More than 50% of small businesses close within 6 months of a cyber-attack – this could be your Mum, Dad or other family member suffering.

Those of you within the cyber community that frequent the more niche areas of this arena and who have a strong and ethical moral compass should have the desire to provide law enforcement with information to enable action to be taken against those that use their cyber knowledge to hurt others.

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

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

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

Yorkshire & Humber REGIONAL CYBER CRIME UNIT

Online Resources for Self-Development

These are free resources which you can use to test and enhance your skills, either for self development or to see whether you are interested in going down that 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, *CYB001X* a good cyber security introduction. www.edx.org/

Hack the Box
Online platform to test and advance penetration testing and cyber security skills… you'll need some skills to get past the invite challenge and get 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/

YH ROCU Yorkshire & Humber REGIONAL CYBER CRIME UNIT

Useful Resources

Online safety for under 18s, parents and schools:

Get Safe Online - general safety	www.getsafeonline.org
Think U Know – age specific advice	www.thinkuknow.co.uk
Net Aware app, game and site advice	www.net-aware.org.uk
UK Safer Internet Centre – general	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 – data breaches	www.haveibeenpwned.com
National Cyber Security Centre	www.ncsc.gov.uk
Small business infographics	

Useful Apps

YOTI – helps children take down images they may have shared

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)	www.ncsyes.co.uk

YH ROCU Yorkshire & Humber REGIONAL CYBER CRIME UNIT

Resources for Teaching & Development

Cyber Discovery
An annual competition run by HM Government's Cyber Schools programme for students in years 10 – 13. Runs alongside the academic year. www.joincyberdiscovery.com/

Cyber Security Challenge UK
The CSCUK offer a number of teaching resources including lesson plans.
www.cybersecuritychallenge.org.uk/education/schools/teachers

Cyber Centurion
An annual competition run by CSCUK for ages 12-18, challenging teams to solve puzzles, break codes and win cyber challenges. Runs alongside the academic year.
www.cybersecuritychallenge.org.uk/competitions/cybercenturion

Tech Partnership
Online learning resources and challenges which can be used for teaching or simply self development. Includes coding, cyber security and game and app design. Students are awarded challenge badges. Also has section for teacher CPD.
learning.thetechpartnership.com/

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. Earn badges for completed labs, and see where you and your academic institution rank in league tables. www.digitalcyberacademy.com/

Cyber First
Nationwide workshops for students run by GCHQ and the National Cyber Security Centre during academic holidays. Tiered by age. Also runs a bursary scheme for university students including summer work experience and a post-graduation employment scheme, and an apprenticeship scheme with GCHQ. www.ncsc.gov.uk/information/cyberfirst-courses
www.gchq-careers.co.uk/early-careers/cyberfirst.html

STEM Net
The STEM network offer lots of free teaching plans including a lesson plan centred on the Computer Misuse Act which links with the CSCUK. www.stem.org.uk/

Computing At School
A national initiative to help teachers provide excellent teaching around computing. Your regional hub can connect you with experts and provide CPD to enhance your skills.
www.computingatschool.org.uk/

Code Monkey
Classroom teaching resource for learning games development www.playcodemonkey.com/

YH ROCU Yorkshire & Humber REGIONAL CYBER CRIME UNIT

Questions to help our understanding

You may be encountering people who have an aptitude towards computing, particular skills or disclose to you that they are involved in online activity that concerns you. We can help. Before contacting us it would be beneficial if you can explore the following questions. Your answers will help us assess the risk to the person caused by their on-line activity and so enable the appropriate safeguarding resources to be made available, along with the right diversions or information:

Motivations and Influences

- What interests you about computers?
- Do you have any interest in a career involving computers?

Computer Skills

- How would you rate your computer skills (1 – useless to 10 – outstanding)?
- Can you write any computer code? If yes:
- Which programming languages can you use?
- Can you create apps or games?
- Tell me about your best computing achievement?

Computer Equipment

- What computers do you have access to (e.g. desktop, laptop, smartphone, tablet, server)?
- What operating systems do you use?
- What VPN (Virtual Private Network) do you use?

Online Activity

- What forums do you look at?
- What social media are you on?
- Do you have favourite usernames or tags?

Understanding of the Law

- Do you have any understanding of the Computer Misuse Act?
- If you think you have ever broken the law online would you like some guidance?

Neurodiversity

- Have you ever been diagnosed with Autism Spectrum Disorder or do you consider yourself to be on the Autism Spectrum?

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

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

Yorkshire & Humber
YH ROCU REGIONAL CYBER CRIME UNIT