

CYBER PROTECT

Hayley Whitbread

ERSOU Cyber Protect
Coordinator



CYBERCRIME

Cyber-Enabled



Cyber-Dependent



CYBERCRIME IN THE EAST

NUMBER OF REPORTS

4,126

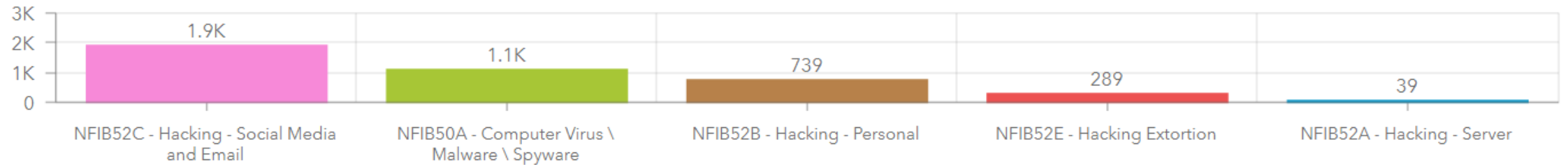
Last update: a few seconds ago

REPORTED LOSSES

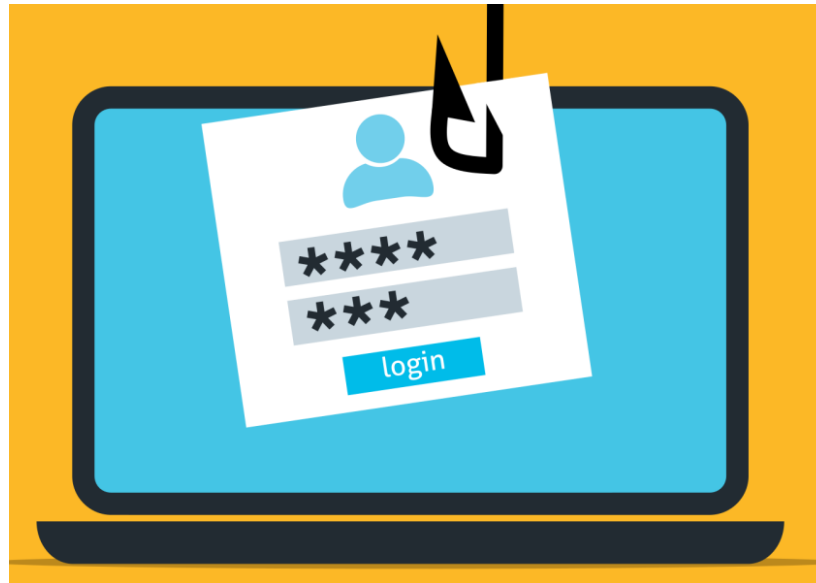
£331.1K

Last update: a few seconds ago

TOP 5 REPORTED CRIME CODES



PHISHING




“**Phishing** is a type of **social engineering attack** in which cyber criminals trick victims into handing over **sensitive information** or **installing malware**.”

SIGNS OF PHISHING

From: MSteam-Outlook Message Center <no-reply@office365protectionservices.co.uk>
Sent: 19 September 2018 11:44
To: Bob Smith <Bob.Smith@Company.com>
Subject: Account Verification

This mail is from a trusted sender.

 **Outlook**

Threat
We're having trouble verifying your Office365 account: Bob.Smith@Company.com on our server, most features will be turned off.
To help prevent account malfunctions, please log into your account portal to verify your account.

Spelling mistakes

[SIGN IN TO MICROSOFT ACCOUNT PORTAL](#)

Note : Outlook will automatically fix your account after this process on the microsoft server and all account features will be turned back on

Thanks for using office365 , we hope to continue serving you.

Microsoft Corpration
One-Microsoft Way Redmond
WA, 98052
All Right Reserved | Acceptable Use Policy | Privacy Notice

Fake domain

Grammatical errors

Fake email signature

REPORT PHISHING



Phishing attacks Dealing with suspicious emails

Phishing emails try to convince users to click on links to dodgy websites or attachments, or to give sensitive information away (such as bank details). This advice includes tips about how to spot the most obvious signs of phishing, and what to do if you think you've clicked a bad link. For more information, please visit www.ncsc.gov.uk/phishing.



What is phishing?

Phishing is when criminals attempt to trick people into doing 'the wrong thing', such as clicking a link to a dodgy website.

Phishing can be conducted via a text message, social media, or by phone, but the term 'phishing' is mainly used to describe attacks that arrive by email.

Criminals send phishing emails to **millions of people**, asking for sensitive information (like bank details), or containing links to bad websites. Some phishing emails may contain viruses disguised as harmless attachments, which are activated when opened.

© Crown Copyright 2020

Make yourself a harder target

Information from your website or social media accounts leaves a 'digital footprint' that can be exploited by criminals. You can make yourself less likely to be phished by doing the following:



Criminals use publicly available information about you to make their phishing emails appear convincing. **Review your privacy settings**, and think about what you post.



Be aware what your friends, family and colleagues say about you online, as this can also reveal information that can be used to target you.



If you have received an email which you're not quite sure about, **forward it to the NCSC's suspicious Email Reporting Service (SERS): report@phishing.gov.uk**

What to do if you've already clicked?

The most important thing to do is not to panic. There are a number of practical steps you can take:



Open your antivirus (AV) software, and run a full scan. Follow any instructions given.



If you've been tricked into providing your password, you should **change your passwords on all your other accounts**.



If you have lost money, you need to report it as a crime to Action Fraud. You can do this by visiting www.actionfraud.police.uk.

Tell tale signs of phishing

Spotting a phishing email is becoming increasingly difficult, and even the most careful user can be tricked. Here are some tell tale signs that could indicate a phishing attempt.



Is the email addressed to you by name, or does it refer to 'valued customer', or 'friend' or 'colleague'? This can be a sign that the sender does not actually know you, and that it is part of a phishing scam.



Others will try and create official-looking emails by including logos and graphics. Is the design (and quality) what you'd expect?



Does the email contain a veiled threat that asks you to act urgently? Be suspicious of words like 'send these details within 24 hours' or 'you have been a victim of crime, click here immediately'.



Look at the sender's name and email address. Does it sound legitimate, or is it trying to mimic someone you know?



Your bank (or any other official source) should never ask you to supply personal information in an email. **If you need to check, call them directly.**



If it sounds too good to be true, it probably is. It's most unlikely that someone will offer you designer trainers for £10, or codes to access films for free.

www.ncsc.gov.uk [@NCSC](https://twitter.com/NCSC) [National Cyber Security Centre](https://www.facebook.com/NationalCyberSecurityCentre) [@cyberhq](https://www.instagram.com/cyberhq)

Emails →
report@phishing.gov.uk

Texts →
7726

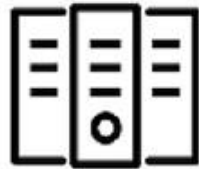
RANSOMWARE



“Ransomware is a malicious software that prevents you from accessing your computer (or the data stored on your computer)”

SHOULD I PAY A RANSOM?

Your computer has been infected!



Your documents, photos,
databases and other important files
encrypted



To decrypt your files you need to
buy our special software -
██████████-Decryptor



Follow the instructions below. But
remember that you do not have
much time

██████████-Decryptor price

You have **6 days, 23:59:40**

- * If you do not pay on time, the price will be doubled
- * Time ends on Jul 9, 19:09:53

Current price **213.23496134 XMR**
≈ 44,999 USD

After time ends **426.46992268 XMR**
≈ 89,998 USD

Monero address: ██████████

* XMR will be recalculated in 5 hours with an actual rate.

CYBER AWARE

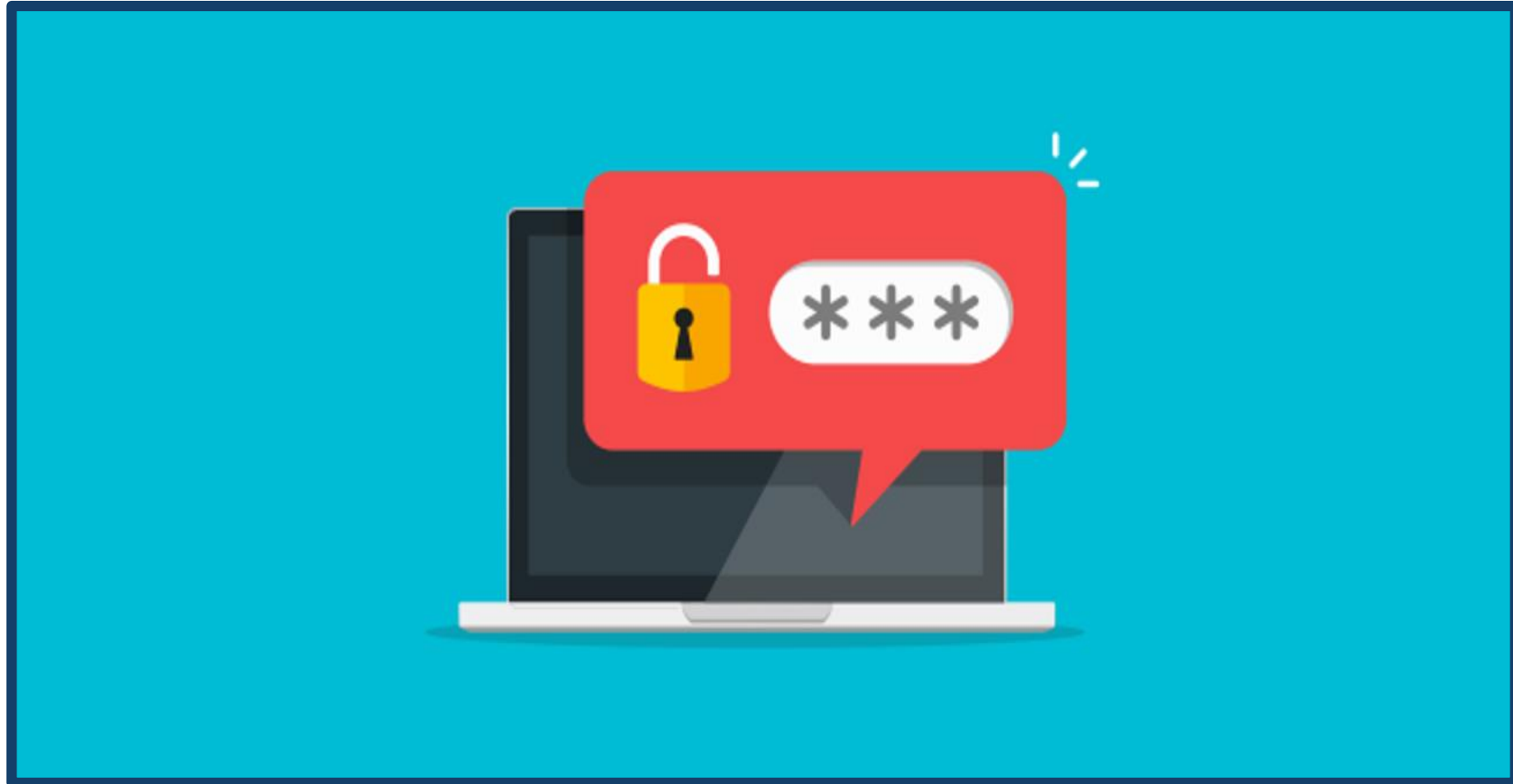


National Cyber
Security Centre

Cyber Aware



EMAIL PASSWORDS



THREE RANDOM WORDS



Three random word passwords.
Simple to make,
tough to break.

 National Cyber Security Centre
a part of GCHQ

 Cyber Aware

<https://www.security.org/how-secure-is-my-password/>

SAVE PASSWORDS TO BROWSER

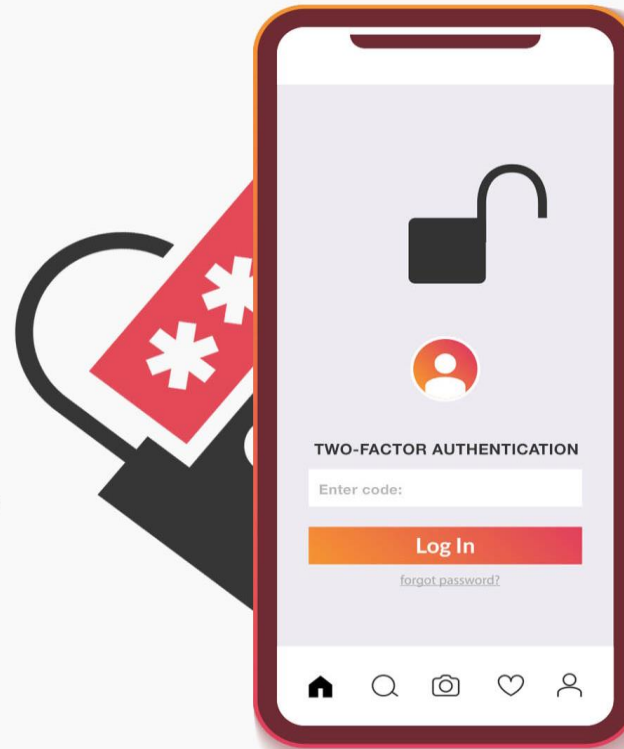


TWO-FACTOR AUTHENTICATION

#2FACTOR

Two-factor authentication

Two-factor authentication (2FA) can help protect your online accounts, even if your password is stolen. You should enable it on your important accounts, such as your email. For instructions on how to set it up, visit www.telesign.com/turnon2fa/tutorials



UPDATE YOUR DEVICES

ActionFraud
National Fraud & Cyber Crime Reporting Centre
actionfraud.police.uk

**Cyber
Aware** 

Protect your devices with the latest software updates

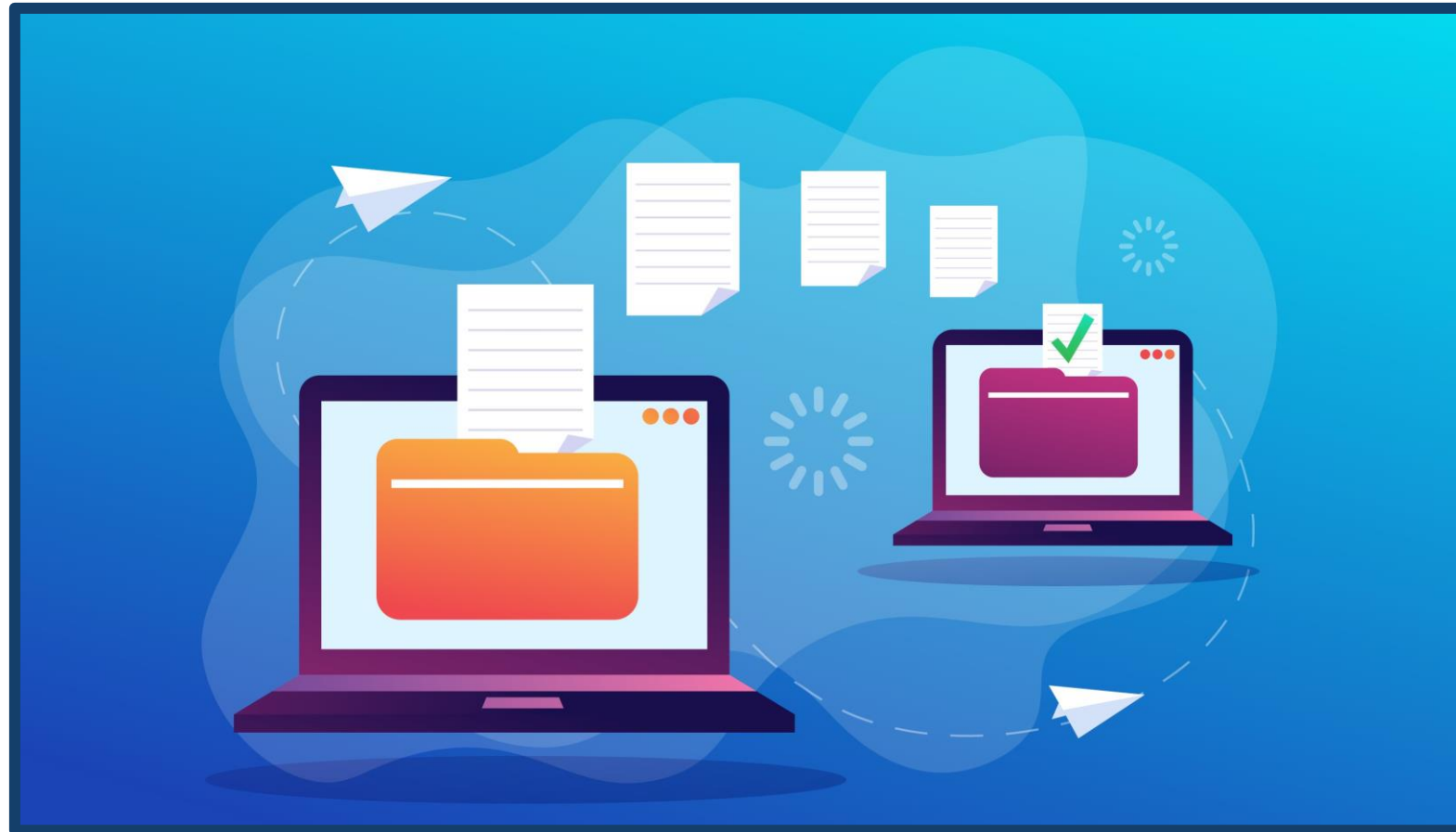
Software updates help keep hackers out

Out-of-date software, apps, and operating systems contain weaknesses. This makes them easier to hack. Companies fix the weaknesses by releasing updates. When you update your devices and software, this helps to keep hackers out.

Automatic updates

Turn on automatic updates for your devices and software that offer it. This will mean you do not have to remember each time.

BACK-UP YOUR DATA



CYBER ACTION PLAN



The screenshot shows the Cyber Aware website interface. At the top left is the 'Cyber Aware' logo with a padlock icon. The main heading is 'Create your Cyber Action Plan', followed by the subtext 'Personalised cyber security advice for sole traders and micro businesses.' Below this are two cards. The left card is titled 'For sole traders & small businesses' and includes the text 'Takes 3-5 mins' and a purple 'Start now' button. The right card is titled 'For individuals & families' and includes the text 'Coming soon'.

Cyber Aware 

Create your Cyber Action Plan

Personalised cyber security advice for sole traders and micro businesses.

For sole traders & small businesses
Takes 3-5 mins
[Start now](#)

For individuals & families
Coming soon

<https://www.ncsc.gov.uk/cyberaware/actionplan>

TOP TIPS FOR STAFF



Stay Safe Online Top tips for staff

Regardless of the size or type of organisation you work for, it's important to understand **why** you might be vulnerable to cyber attack, and **how** to defend yourself. The advice summarised below is applicable to your working life and your home life. You should also familiarise yourself with any cyber security policies and practices that your organisation has already put in place.

Who is behind cyber attacks?

Online criminals

Are really good at identifying what can be monetised, for example stealing and selling sensitive data, or holding systems and information to ransom.



Foreign governments

Generally interested in accessing really sensitive or valuable information that may give them a strategic or political advantage.

Hackers

Individuals with varying degrees of expertise, often acting in an untargeted way – perhaps to test their own skills or cause disruption for the sake of it.



Political activists

Out to prove a point for political or ideological reasons, perhaps to expose or discredit your organisation's activities.

Terrorists

Interested in spreading propaganda and disruption activities, they generally have less technical capabilities.



Malicious insiders

Use their access to an organisation's data or networks to conduct malicious activity, such as stealing sensitive information to share with competitors.

Honest mistakes

Sometimes staff, with the best of intentions just make a mistake, for example by emailing something sensitive to the wrong email address.



Defend against phishing attacks

Phishing emails appear genuine, but are actually fake. They might try and trick you into revealing sensitive information, or contain links to a malicious website or an infected attachment.



Phishers use publicly available information about you to make their emails appear convincing. **Review your privacy settings**, and think about what you post.



Know the techniques that phishers use in emails. This can include urgency or authority cues that pressure you to act.



Phishers often seek to exploit 'normal' business communications and processes. **Make sure you know your organisation's policies** and processes to make it easier to spot unusual activity.



Anybody might click on a phishing email at some point. If you do, **tell someone immediately** to reduce the potential harm caused.

Secure your devices

The smartphones, tablets, laptops or desktop computers that you use can be exploited both remotely and physically, but you can protect them from many common attacks.



Don't ignore software updates - they contain patches that keep your device secure. Your organisation may manage updates, but if you're prompted to install any, make sure you do.



Always lock your device when you're not using it. Use a PIN, password, or fingerprint/face id. This will make it harder for an attacker to exploit a device if it is left unlocked, lost or stolen.



Avoid downloading dodgy apps. Only use official app stores (like Google Play or the Apple App Store), which provide some protection from viruses. Don't download apps from unknown vendors and sources.

Use strong passwords

Attackers will try the most common passwords (e.g. password1), or use publicly available information to try and access your accounts. If successful, they can use this same password to access your other accounts.



Create a strong and memorable password for important accounts, such as by using three random words. Avoid using predictable passwords, such as dates, family and pet names.



Use a separate password for your work account. If an online account gets compromised, you don't want the attacker to also know your work password.



If you write your passwords down, store them securely away from your device. Never reveal your password to anyone; your IT team or other provider will be able to reset it if necessary.



Use two factor authentication (2FA) for important websites like banking and email, if you're given the option. 2FA provides a way of 'double checking' that you really are the person you are claiming to be when you're using online services.

If in doubt, call it out

Reporting incidents promptly - usually to your IT team or line manager - can massively reduce the potential harm caused by cyber incidents.



Cyber attacks can be difficult to spot, so don't hesitate to ask for further guidance or support when something feels suspicious or unusual.

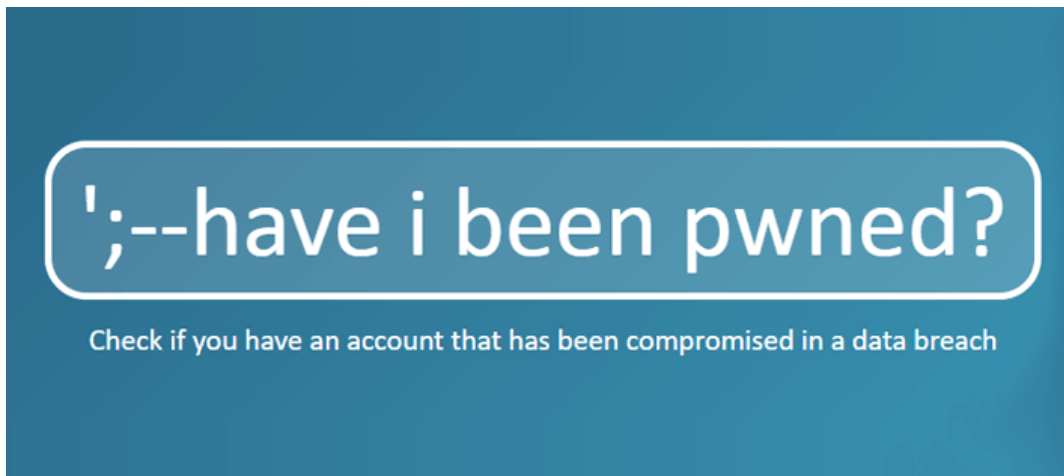


Report attacks as soon as possible - don't assume that someone else will do it. Even if you've done something (such as clicked on a bad link), always report what's happened.

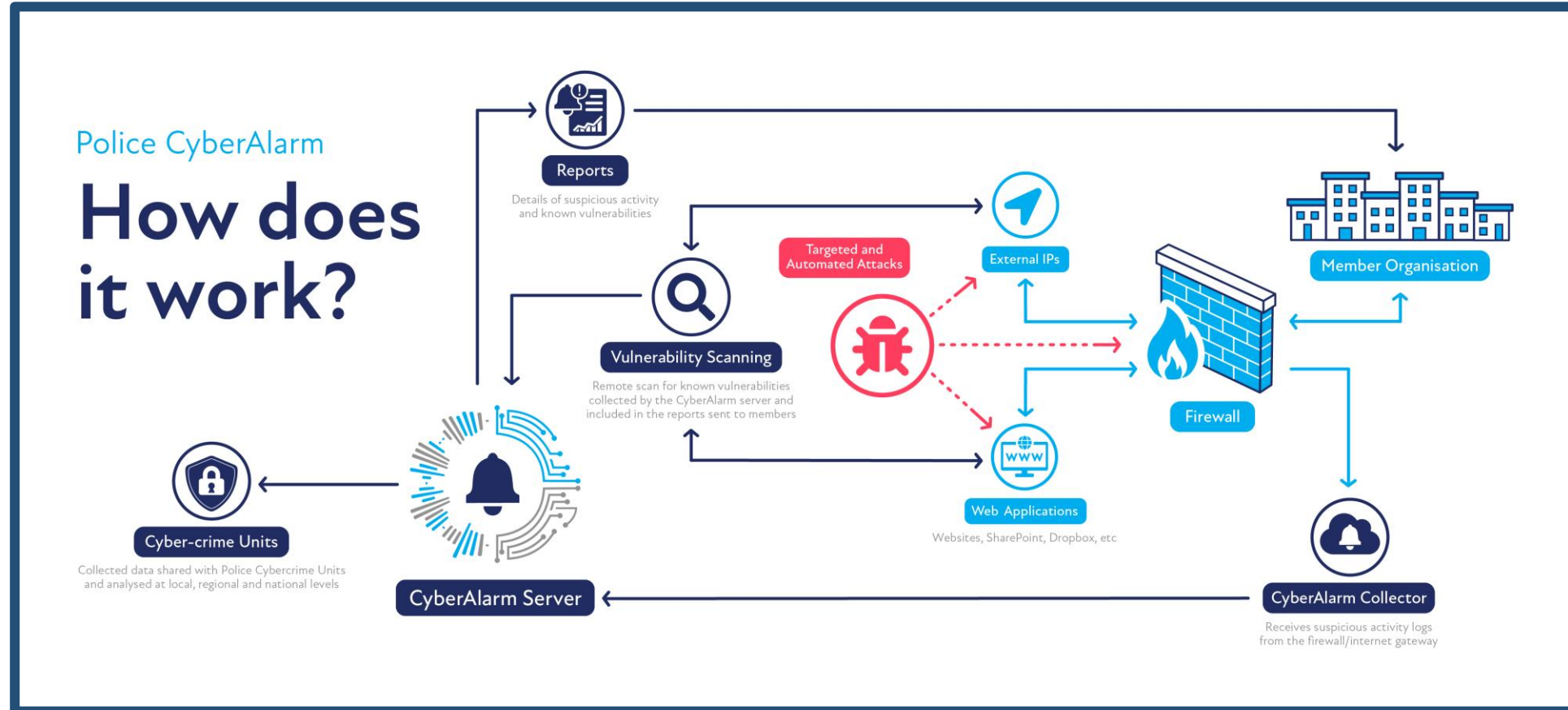


Don't be afraid to challenge policies or processes that make your job difficult. Security that gets in the way of people doing their jobs, doesn't work.

USEFUL RESOURCES



POLICE CYBERALARM



<https://www.cyberalarm.police.uk/>

QUESTIONS

Hayley Whitbread
ERSOU Regional Cyber Protect Coordinator

cyberprotectersou@beds.police.uk





CYBER CHOICES

Preventing individuals from becoming involved in cyber dependent crime
Helping them make the right #CyberChoices

Steph Frankish
Regional Cyber Choices Co-Ordinator

www.cyberchoices.uk

Aims of the Cyber Choices Programme

Explain the difference between legal and illegal cyber activity

Encourage individuals to make informed choices about their use of technology

Increase awareness of the Computer Misuse Act 1990

Promote positive, legal cyber opportunities

Regional Cyber Choices Network

- Cyber Choices is a programme delivered by the Regional & Local Cyber Choices Network, co-ordinated by the National Crime Agency.
- We have 10 Regional Organised Crime Units and 43 Local Police Forces with dedicated Cyber Choices Officers.
- All officers are capable of identifying vulnerable young people in their jurisdiction for Cyber Choices interventions.
- Take a look to see who covers your area.



- 1: North East (NERSOU)
- 2: Yorkshire & Humber (YHROCU)
- 3: North West (NWROCU)
- 4: South Wales (TARIAN)
- 5: West Midlands (WMROCU)
- 6: East Midlands (EMSOU)
- 7: Eastern (ERSOU)
- 8: South West (SWROCU)
- 9: London (MPS)
- 10: South East (SEROCU)

3% of teens are likely to smoke, 2% of teens are likely to have sex and 2% of teens are likely to be in a gang.

What percentage of teens are likely to hack?

5%

What percentage of teens admitted to trying to compromise someone else's account (social media or similar)?

25% or 1 in 4

**What percentage of hackers started before the
age of 16?**

61%

Aims of the Cyber Choices Programme

The average age of someone arrested for drugs trafficking and similar is around 37

What is the average age of someone arrested for cyber dependent crimes?

17

Answers in the chat!!

Achieving our Aims



ENGAGE & EDUCATE

Welcome to CyberLand

Try our game below or click the button to see all of our games.

The games are currently not supported on mobile devices.

See Games

IDENTIFY, INTERVENE & INSPIRE

This is CyberLand.


Each building with a arrow above it has a set of activities to test your knowledge and skills.

Each activity will score you points. After you have attempted all of the activities you will receive a code word based on your final score.

Your scores will be shown in the top left of the map screen. As you complete tasks, the arrows above the associated building will turn green.

All the tasks must be completed in one sitting to generate a code at the end for entry into the competition. You can replay the game as many times as you like to improve your end score!

Achieving our Aims



Giving presentations, for example at school assemblies, youth clubs or conferences



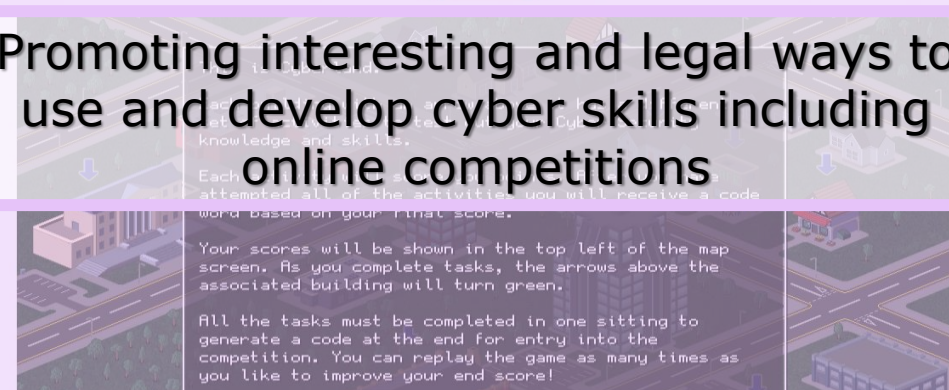
Attending events such as gaming and computer exhibitions

Welcome to CyberLand

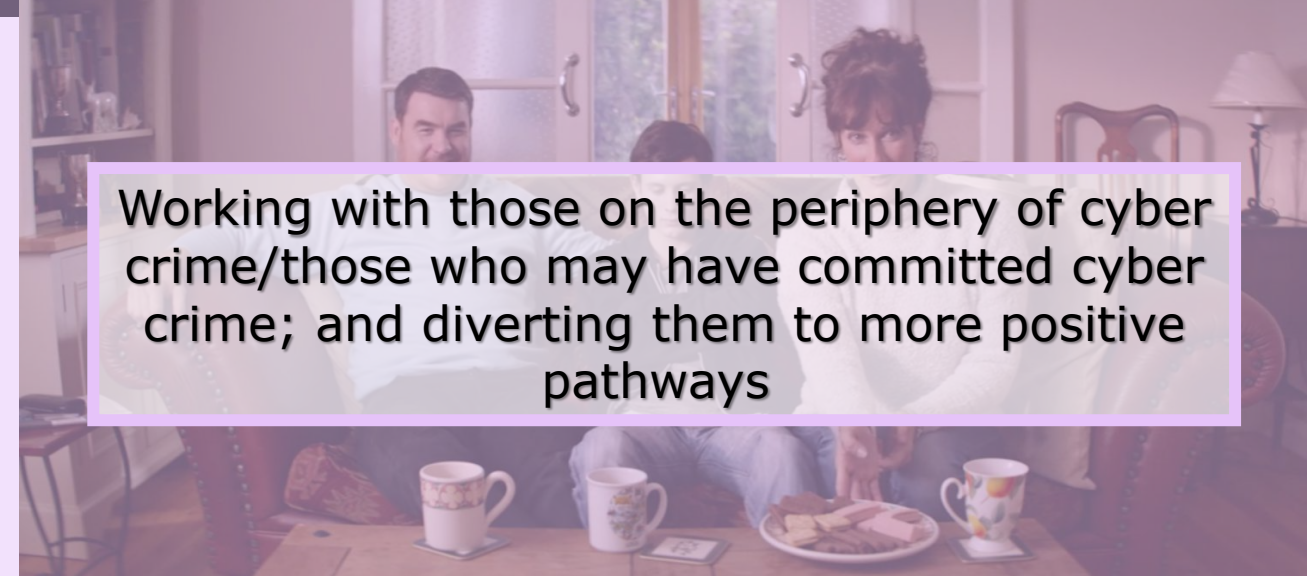
Try our game below or click the button to see all of our games.

The games are currently not supported on mobile devices.

See Games



Promoting interesting and legal ways to use and develop cyber skills including online competitions



Working with those on the periphery of cyber crime/those who may have committed cyber crime; and diverting them to more positive pathways

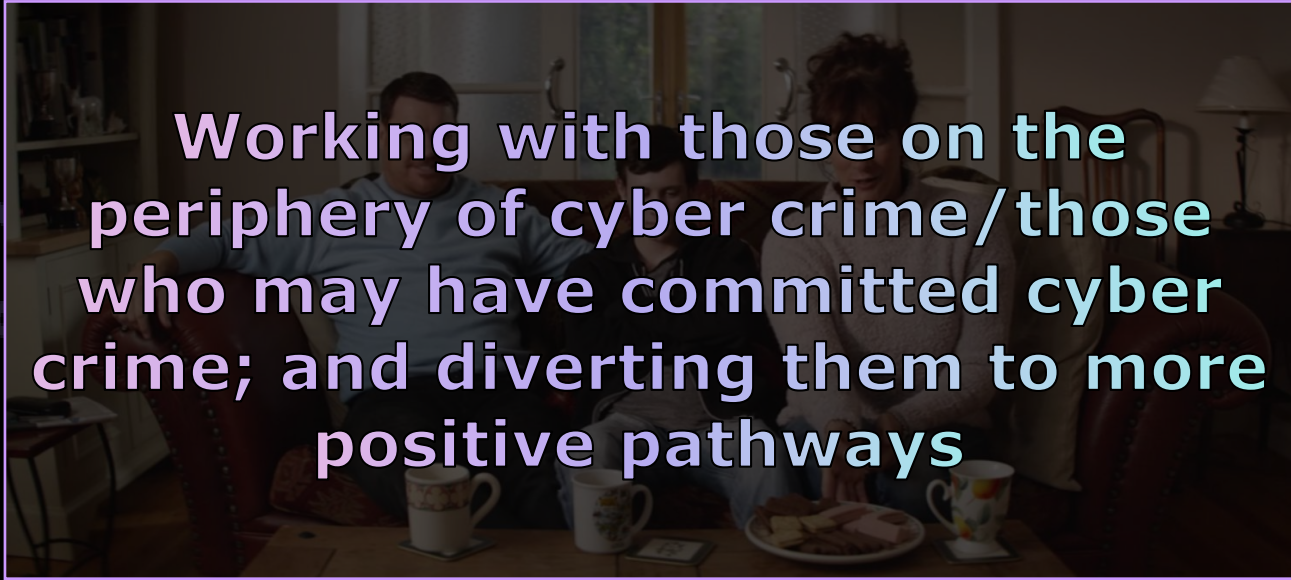


**CYBER
CHOICES**

Referral

www.cyberchoices.uk

Referrals Outline



Working with those on the periphery of cyber crime/those who may have committed cyber crime; and diverting them to more positive pathways

Referral Examples:

- Teachers
- Social Services
- Parents
- Police Investigations
- Public events

Are they suitable for Cyber Choices?

Action:

- Ensure knowledge and understanding of CMA (1990)
- Ensure knowledge of consequences
- Positive interventions
- Signpost to resources

Vulnerabilities & Commonly seen characteristics;

- **Isolated – online interaction**
- **Computer/gaming pre-occupation**
- **Ignorance of wider impact of actions**
- **Neurodiversity**

By-passing firewall or parental controls

- School / College
- Home

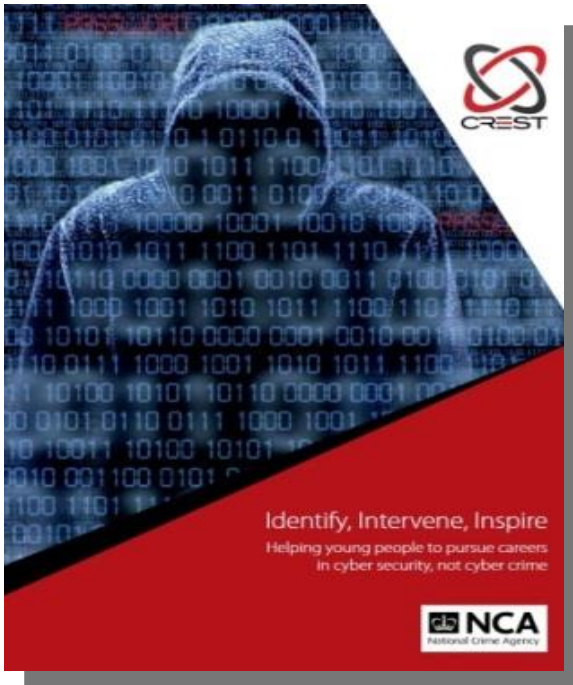
Network Intrusion

- Privilege escalation
- Non-technical password guessing or use
- Remote Access Tools / Trojans

DDoS tools

- Purchase of service
- Use of tools

Identify, Intervene, Inspire Report



- Published in February 2016
- Information from 2015 workshop with penetration testers
- Compared profiles of cyber criminals and top level penetration testers to identify commonalities and differences which could identify causes of deviance.

1)
Documented gaming cyber crime pathway and possible intervention points.

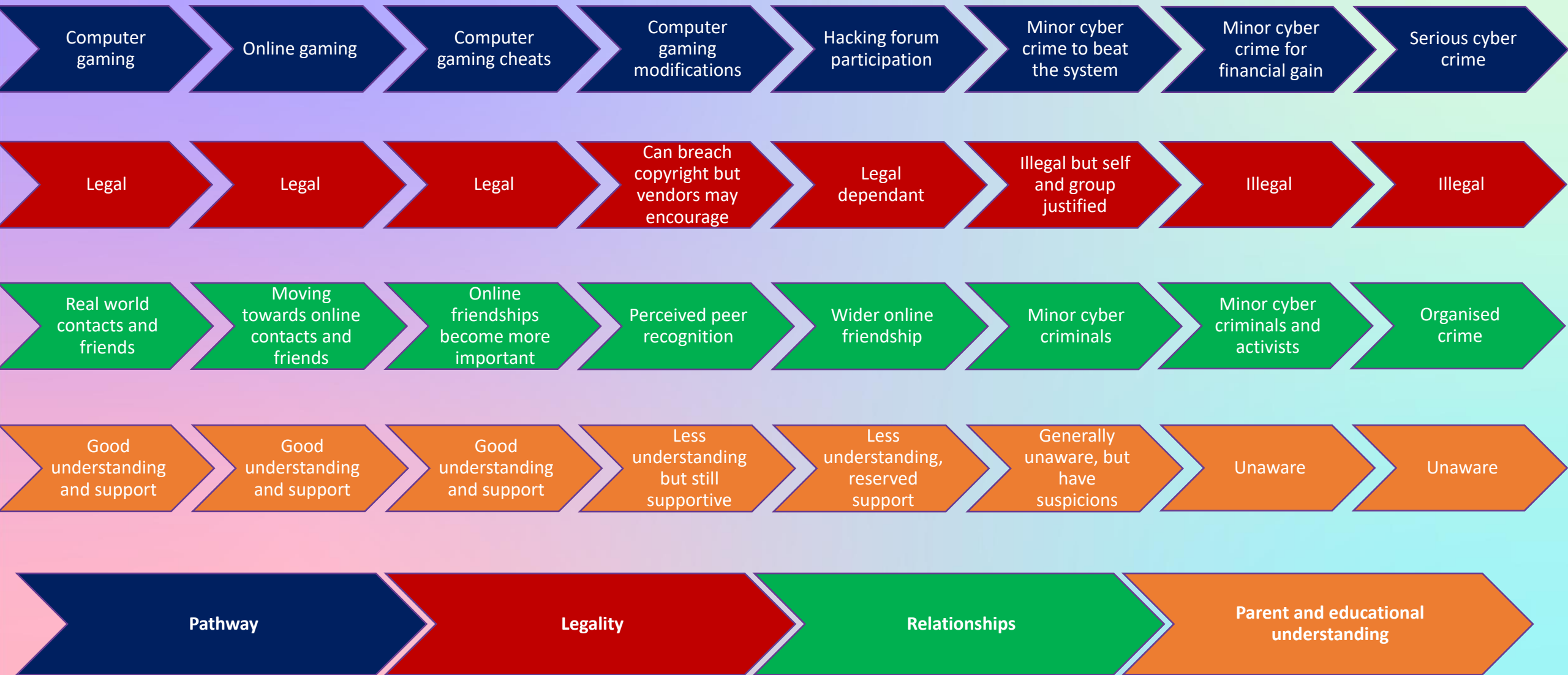
...It is important to remember that not all gamers are cyber criminals and not all cyber criminals are gamers.

2)
Re-enforced that financial gain is not the primary motivation for target audience. Challenge and peer recognition are more important.

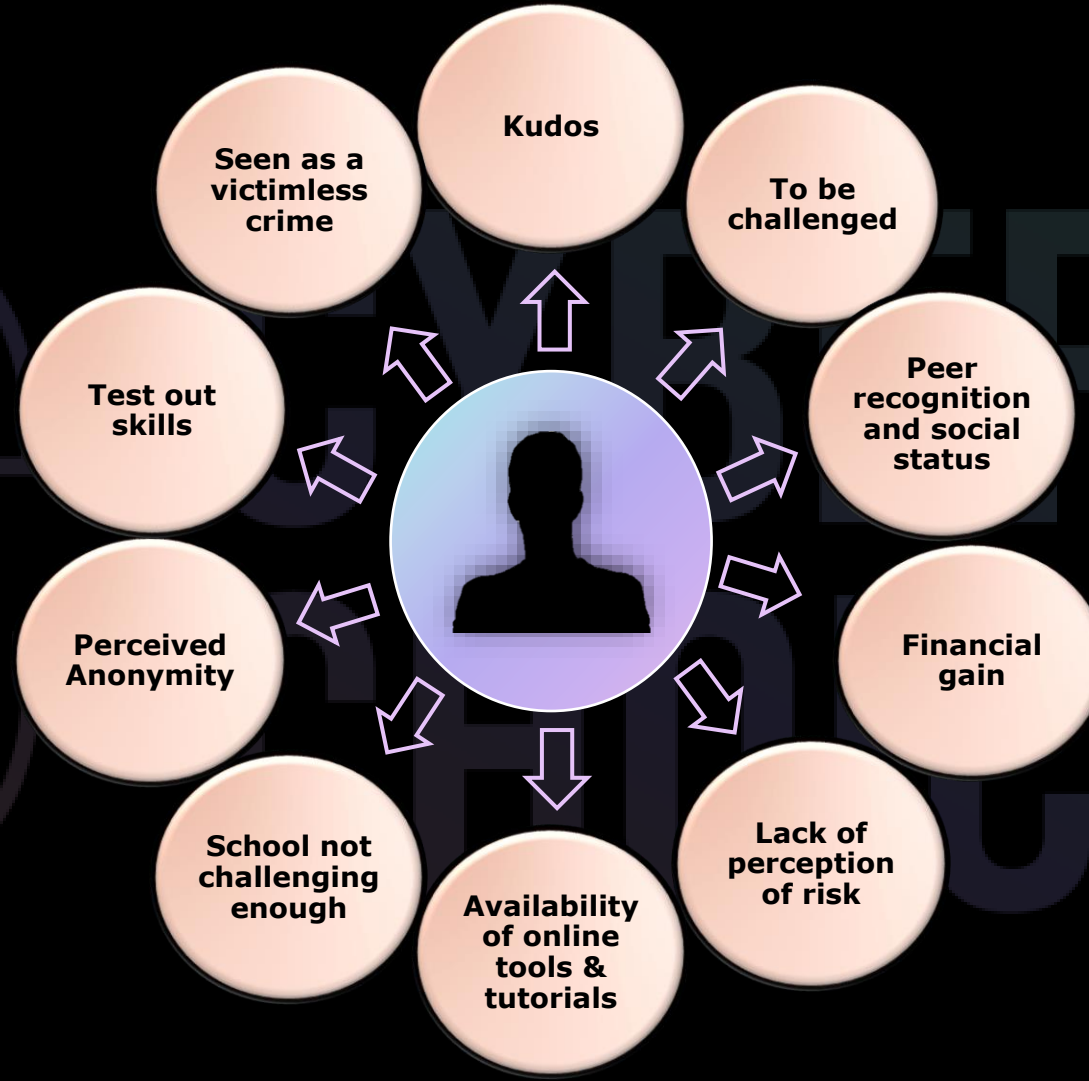
3)
Introduction to positive interventions as a cyber prevention technique.

The earlier the intervention, the more likely a positive outcome.

Cyber Criminal Career Pathway – Gaming Pathway



Motivations





CYBER CHOICES

LEGISLATION

www.cyberchoices.uk

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 access with intent to impair, or with recklessness as to impairing, operation of a computer.

Section 3A:

Making supplying or obtaining articles for use in another Computer Misuse Act offence.

Section 3ZA:

Unauthorised acts causing, or creating risk of serious damage.

Section 2 Bedford example

A Bedford School boy realised that everybody was given a default password at the beginning of term including teachers, he experimented logging into a teachers account and he proceeded to manipulate data. Deleting merits and creating detentions.

This ended in him being referred to us for words of advice

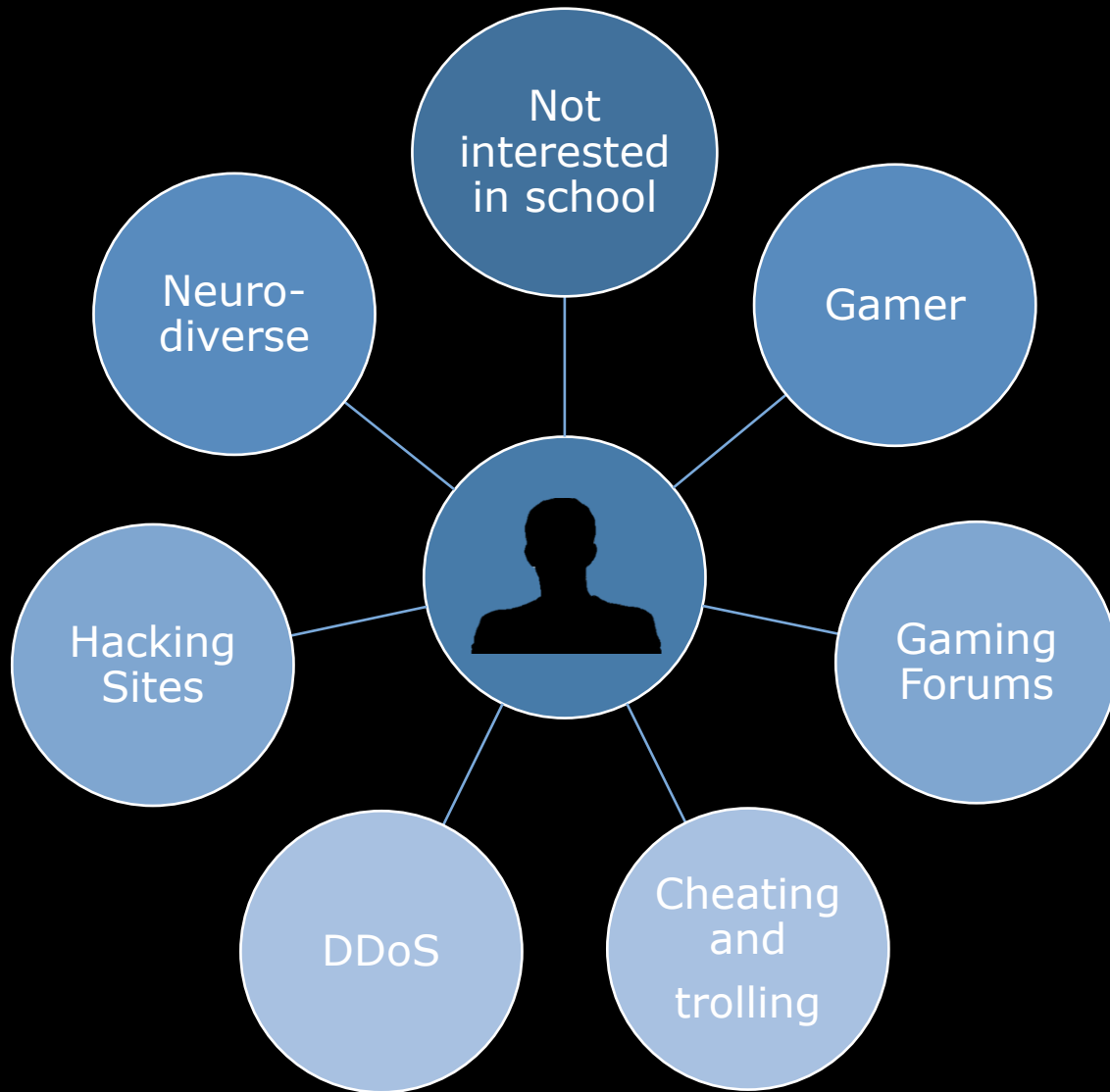
Section 3 and 3a Norfolk example

A school boy from Norfolk was annoyed at his school and decided to DDoS his schools systems taking them offline.

What he didn't realise was that their system was managed by an IT management company who managed multiple other businesses, schools, GP surgeries in the local area which were all also taken out with his DDoS attack.

He ended up with a conditional caution for this and a condition of this was to work with Cyber Choices.

Case Study section 3 and 3a Hertfordshire



Aged 15

- Programmed own DDoS software

Aged 16

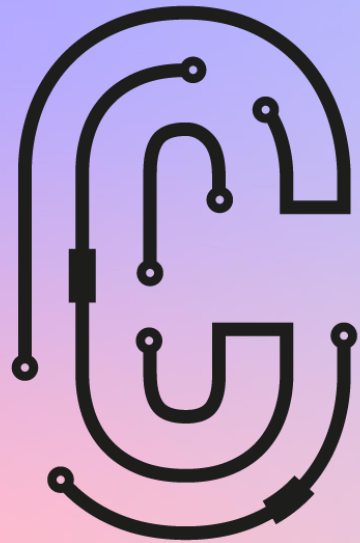
- Commercialised software
- Software developed over 110,000 users
- Software generated 1.7 million attacks

Aged 16-18

- Committed nearly 600 attacks against over 180 IP addresses

Aged 18

- Arrested
- Found with over £350,000 and nearly 250 Bitcoin
- Tried as Juvenile
- 24 months imprisonment



CYBER CHOICES

RESOURCES

www.cyberchoices.uk

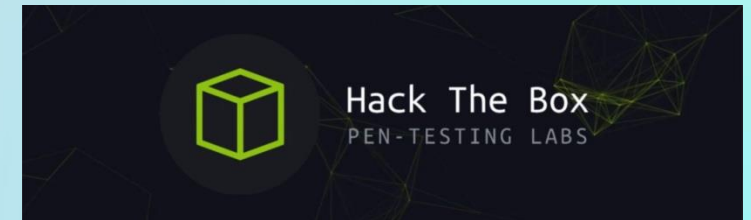
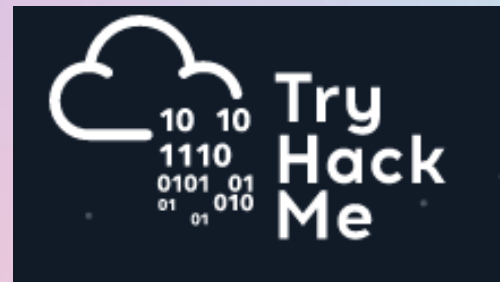
Resources



CYBRARY



freeCodeCamp (🔥)



Keeping children safe in education 2021

Statutory guidance for schools and
colleges

September 2021

KCSIE

Annex B – Further Information
Page 127-128 - Cybercrime

If there are concerns about a child in this area, the designated safeguarding lead (or a deputy), should consider referring into the **Cyber Choices** programme. This is a nationwide police programme supported by the Home Office and led by the National Crime Agency, working with regional and local policing. It aims to intervene where young people are at risk of committing, or being drawn into, low level cyber-dependent offences and divert them to a more positive use of their skills and interests.

Resources for Schools – Barefoot Computing - Primary



WHO DOES THIS BELONG TO?

Age: 6-7 years

Concepts & Approaches:

Collaborating, Evaluation

Curriculum Links:

PHSE, Digital literacy

Focusing on ownership and use of everyday objects this lesson helps children understand ownership and permissions which are the basics of the ethical use of computers.



YOU'RE THE JURY

Age: 7-9 years

Concepts & Approaches:

Abstraction, Algorithms, Collaborating, Creating, Decomposition, Evaluation, Logic

Curriculum Links:

PHSE, Digital literacy

Turning the classroom into a courtroom helps pupils to explore the law and consequences of cyber-crime. Role play and scenarios are used to bring this topical subject to life. Extension lessons are included to help showcase learning and share knowledge with others.



YOU'RE THE CYBER SECURITY EXPERT

Age: 9-11 years

Concepts & Approaches:

Algorithms, Decomposition

Curriculum Links:

PHSE, Digital literacy

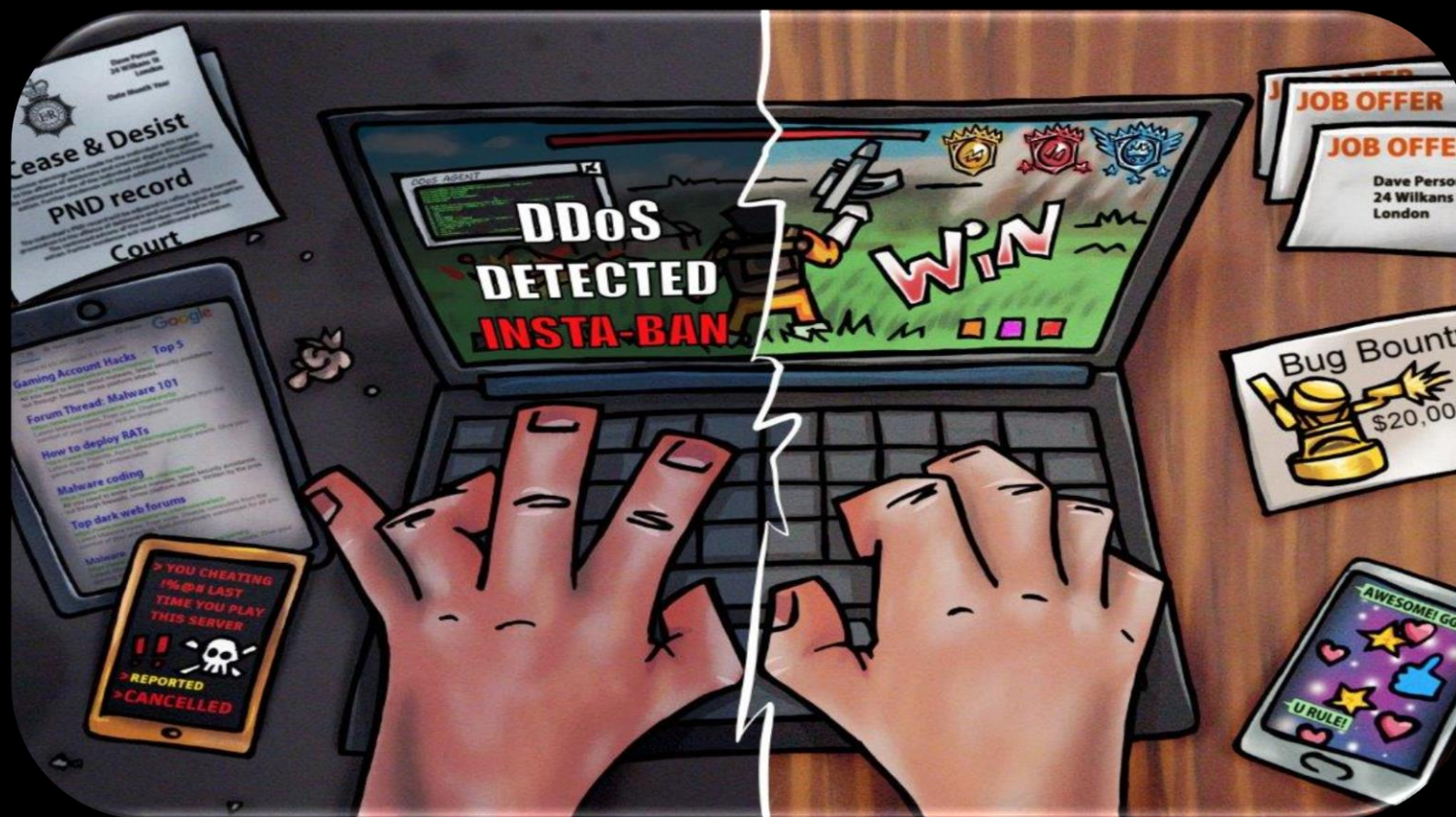
By accepting a challenge from a cyber security expert, the children consider how a criminal might try and discover a secret code for a padlock. Through exploration of a programme they then go on to learn about the use of variables and conditional loops in code, and how to create stronger, more secure pins and passwords.

are

ting.

The Cyber Choices team can arrange or deliver informative presentations in schools, youth groups or other organisations to raise awareness of the Computer Misuse Act and point out positive ways young people can develop cyber skills.

Resources for schools - secondary



PSHE LESSON PLANS (Personal, Social & Economic Education)

Two free Key Stage 3 lesson plans on the causes and effects of cyber crime and how to avoid it.

12-14 year olds

Launched September 2019

[Access on the PSHE website](#)

THANK YOU

Steph Frankish

Eastern Region Cyber Choices Team

cyberprevent@ersou.pnn.police.uk

www.cyberchoices.uk

