Cyber Crime and Online Safety

Niall McNicholas

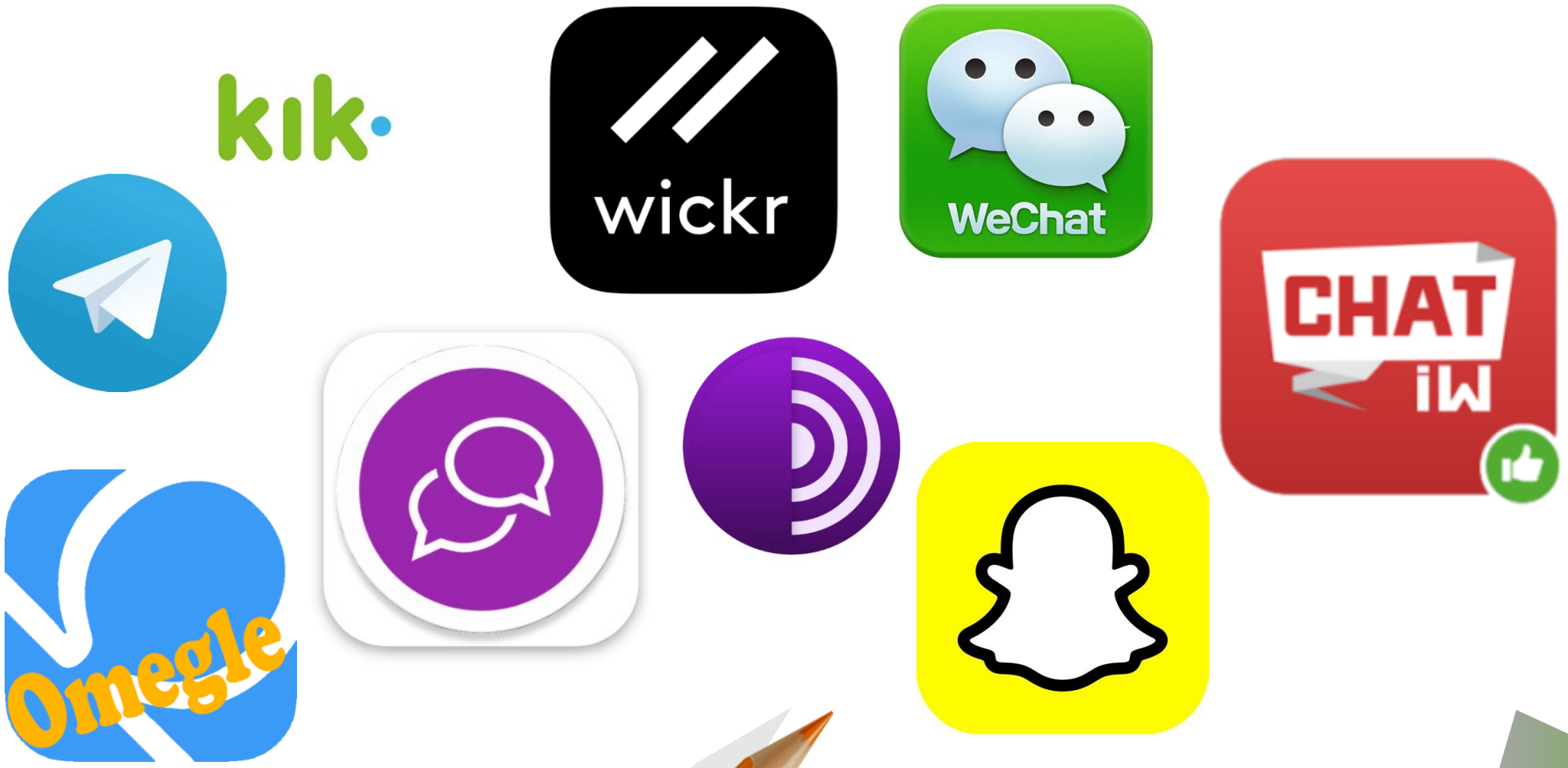
Cyber Dependent Crime Specialist

Cyber and Digital Crime Unit

What we do

- **Prepare** businesses and organisations to effectively deal with cyber incidents
- **Protect** communities from the latest cyber threats
- **Pursue** cyber offenders and bring them to justice
- **Prevent** young people from moving into cyber crime

Social Media



Social Media

Age Restrictions!

Facebook – 13

Snapchat – 13

Instagram – 13

Twitter – 17

YouTube – 13

WhatsApp – 13

Tiktok – 13

ALWAYS SIGN UP WITH YOUR CORRECT AGE

- Don't let people know which school you go to
- Don't talk to strangers, no matter who they say they are.
- If you take a photograph of a friend, always ask them if it's okay to share.
- Don't share where you live or your telephone number

Don't Share!

Having that conversation?

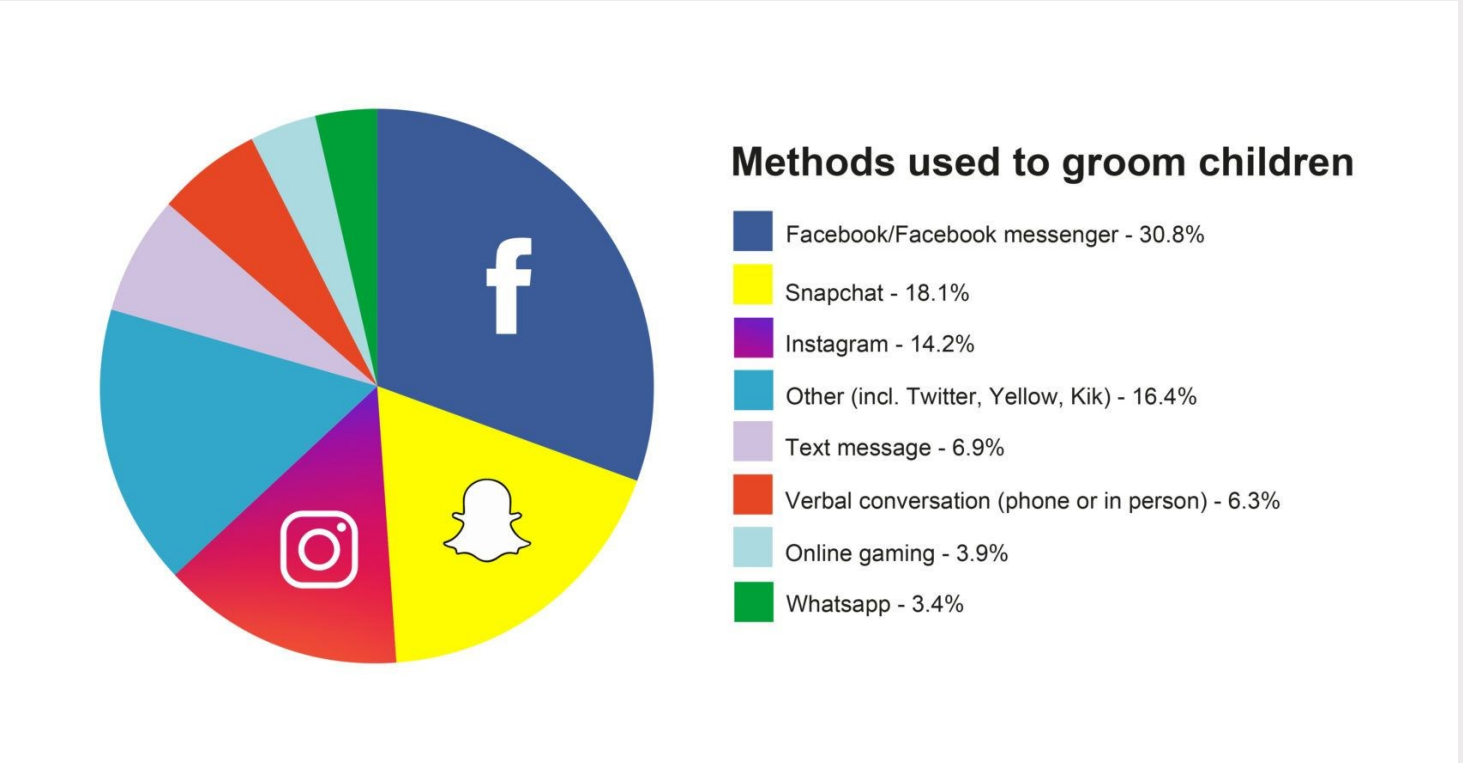
What is Online Grooming?

Online grooming is when someone uses the Internet to trick, force or pressure a young person into meeting them or sending photographs to them.

DO YOU KNOW WHO YOU ARE TALKING TO???
You meet online Susan who claims she is 13 years old from Cumbria. You have arranged to meet her at the park this afternoon.

This is Frank, he is 55 years old and is an online child groomer.

Online Grooming Facts



www.

Online Grooming

Anyone can groom another person.

A 'groomer' is someone who makes an emotional connection with someone to try and make you do things like:

- Have unwanted conversations online or by text messages
- Send embarrassing images of yourself
- Sending videos of yourself
- Do something live on webcam
- Meet up with them in person
- They might be old, or young and any gender

#cyberchoices

Cyber Prevent

- **Deter** individuals from
  - getting involved in cybercrime
  - moving deeper into cybercrime
  - and/or from reoffending
- **Cyber Choices**
  - for all Cyber Prevent public facing activity
  - helps people make positive choices and use their cyber skills in a legal way

www.cyberchoices.uk

Cyber Prevent

- Explain the difference between legal and illegal cyber activity (CMA 1990)
- Encourage individuals to make informed choices about their use of technology
- Deter and/or divert individuals away from cyber crime (such as Cease & Desist)
- Promote legal technology opportunities

Cyber enabled crime

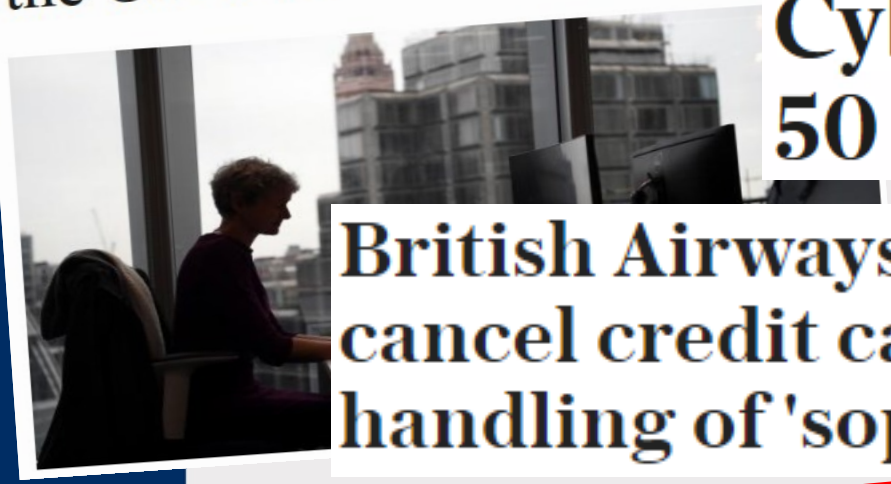
Cyber dependent crime

Cyber-**dependent** Crime

Technology is required to commit the crime

Cyber crime in the news

100 hacker groups are targeting the UK's secrets and economy



17-year-old accused of masterminding Twitter bitcoin scam

Cyberattackers take control of 50 million Facebook accounts

British Airways hacking: Customers cancel credit cards as airline defends handling of 'sophisticated' cyber att...

Barrow computer hacker tapped into school network and brought down Labour website

Bradley Kai Hayden Niblock, 22, was caught after the Cyber and Digital Crime Unit followed a pattern of online offending last year.

Cyber criminal – Bradley Niblock

Targeted a school network as well as a Labour Party website in the road up to an election.

Bradley operated a Twitter profile to flaunt his hacking, which amassed 75,000 followers.

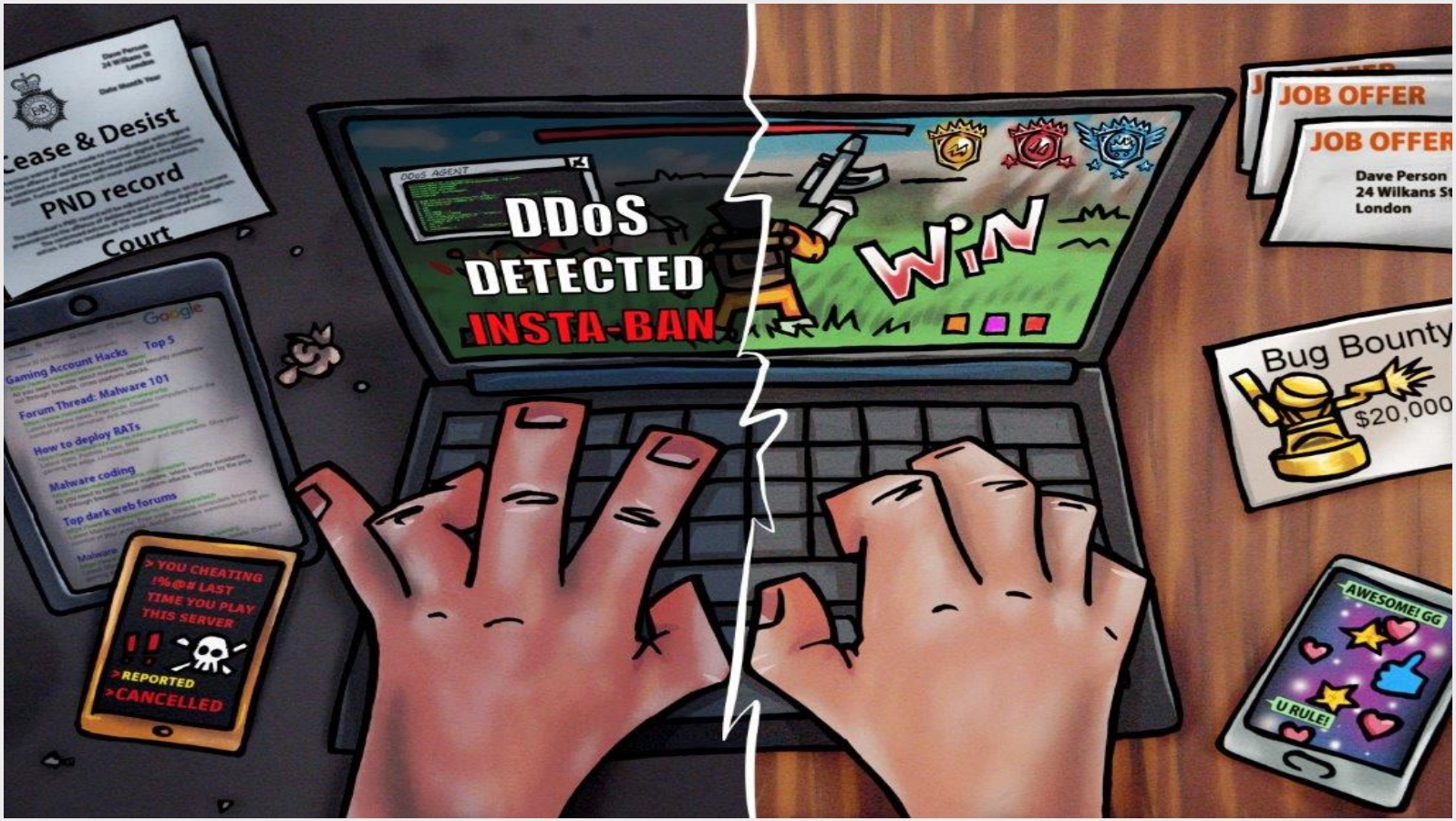
Bradley carried out a Denial of Service attack on the website for the Labour campaign for Barrow at the 2019 General Election.

He used his Twitter platform to orchestrate the attack with other offenders.

Niblock was also found to have unauthorised access to his school networks.

Judge at Preston Crown Court gave Niblock eight month prison sentence, suspended for two years, 200 hours of unpaid work and a 3 year CBO.

Choosing the legal path



To avoid making illegal #CyberChoices, there are <u>FOUR</u> main things to remember…

Choosing the legal path

1

Don’t access anyone else’s computer, device, network or their accounts without their permission

2

Don’t do anything that stops someone else’s computer, network or device working properly, without the owner’s permission

3

Don’t change the way a computer, device, network or website works without the owner’s permission

4

Don’t download, make or supply anything for the purpose of committing cyber crime

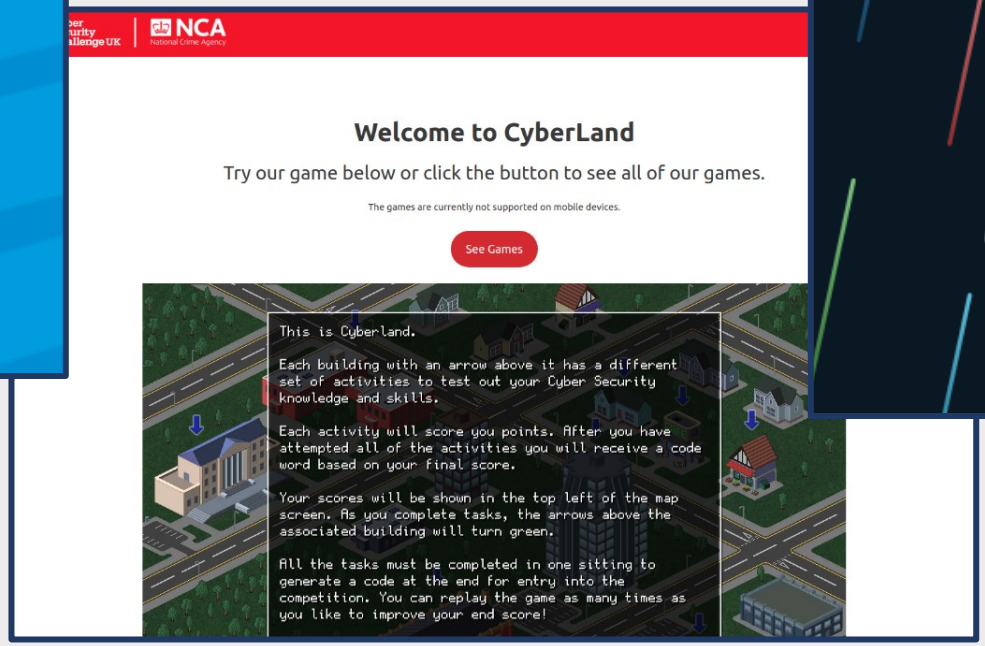
Available educational resources

CoderDojo

{code club}

codecademy

Cyber First



cyber discovery

Referral Process

- Cyber prevent nominals
  - A individual who may be of concern of being involved within cyber criminality
- Cyber Choices Programme
  - Deterrence program set up to engage with an individual to provide a positive diversion into a career using their skills, could include training, education around the laws and possible work experience.
- Intervention tools

Thank you!

cyber@cumbria.police.uk