Cyber PREVENT;

#CyberChoices

Preventing individuals from becoming involved in cyber dependent crime
Working with ROCUs

Yorkshire and the Humber (ODYSSEY)
(TITAN) North West
North East (NEROCU)
(WMROCU) West Midlands
East Midlands (EMSOU)
(TARIAN) Wales
South West (SWROCU)
East of England (ERSOU)
London (FALCON)
South East (SEROCU)
4 Ps

- Prepare
- Pursue
- Protect
- Prevent
Cyber Prevent

• Cyber enabled crime

• Cyber dependent crime
Cyber Prevent Aims

To deter individuals from getting involved in cyber dependent crime, and prevent re-offending.

To understand behaviours and motivations behind offending.

To promote legal and ethical use of skills, including opportunities in cybersecurity.
Rationale

• Average age of cyber dependent offenders at arrest? 17

• 1 – 2 years investigation in some cases

Primary school children in South Yorkshire are being sucked into involvement in serious computer crimes, The Star can reveal. On six occasions in the past three years, South Yorkshire Police have dropped cyber crime investigations after discovering suspects in their cases were under ten years old, which is the age of criminal responsibility.
Rationale

- Perceived online anonymity
- Little or no knowledge of the law
- Motivations is the challenge rather than financial gain
- Wouldn’t commit ‘conventional’ crime
- Higher than average occurrence of those who identify as on the Autistic spectrum
- Not all technically skilled - ‘Off the shelf’ cyber crime tools & tuition readily available
Understanding the pathways for cybercriminals vs those who went into the cyber security or similar professions CREST / NCA – “Identify, Intervene, Inspire”
Engage & Educate
Identify, Intervene, Inspire
Engage & Educate

- Educational establishments
- STEM events
- Public Events
Identify, Intervene, Inspire

**Identify**

- Referrals from educational establishments and other partners
- Intelligence from Police investigations / operations
- Family referrals at public events
Spotting the Signs

- Already in trouble!
- Focussed interest in computing
- Ahead of peers & tutor and bored in lessons
- Flagged search terms
Spotting the Signs

• Social ‘class’ is irrelevant
• Isolated individual..
• A group interested in hacking or similar
• Predominantly male
• Neurodiversity can be a factor
Identify, Intervene, Inspire

Intervene

• Ensure knowledge and understanding of Computer Misuse Act 1990

• Be clear on consequences of breaking the law

• Relate real world ethics to on-line activities - Social responsibility and real world impact
Identify, Intervene, Inspire

Inspire

- Positive diversions
- Resources that offer ethical and legal ways to pursue skills and interests
- Opportunities
Resources

National  ↔  Regional  ↔  Local
Resources

• NCA website
  • What we do > Cyber Crime > Preventing young people from getting involved

• CREST / NCA Indentify, Intervene, Inspire report

• CMA leaflet
Resources

Don’t get involved in cybercrime

The NCA and Police take cybercrime very seriously. We work with national and international partners to investigate cyber criminals. If you get involved, you could face the following consequences:

- A visit and warning from Police or NCA Officers
- Being arrested
- Having your computer seized and Internet access restricted
- Paying a penalty or fine
- A significant prison sentence

A permanent criminal record could affect education and future career prospects, as well as overseas travel.

Cybercrime is not a victimless crime. Imagine how you would feel if someone illegally accessed your private and personal information, could control your computer, or stop you using the Internet.

A Guide to the Computer Misuse Act 1990 (CMA)

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

<table>
<thead>
<tr>
<th>Offence</th>
<th>Example of potential unlawful activity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Section 1 &gt; Unauthorised access to computer material</td>
<td>Without their knowledge, you watched your friend put their password into their phone. You then used it to gain access to their phone and downloaded their photos</td>
</tr>
<tr>
<td>Section 2 &gt; Unauthorised access with intent to cause or facilitate commission of further offences</td>
<td>Without their permission, you accessed your friend’s smartphone, obtaining their bank details so you could transfer money from their account</td>
</tr>
<tr>
<td>Section 3 &gt; Unauthorised acts with intent to impede, or with recklessness as to impeding, operation of computer</td>
<td>You used a hacker tool to knock a friend offline from an online game</td>
</tr>
<tr>
<td>Section 3A &gt; Unauthorised acts causing, or creating risk of, serious damage</td>
<td>You hacked into the computer system of a Government Agency and were reckless as to the consequences - National security was undermined</td>
</tr>
<tr>
<td>Section 34 &gt; Making, supplying or obtaining articles for use in another CMA offence</td>
<td>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</td>
</tr>
</tbody>
</table>
Resources

• Digital Defenders booklet
Resources

- #Cyberchoices videos – YouTube
Working with Cyberchoices

https://www.youtube.com/watch?v=DjYrxzSe3DU
Working with Partners

• Engagement with Universities, Colleges, Schools
• Raising awareness of the Referral option to Cyber Prevent
• Engaging with industries and businesses
• Diversions, opportunities, facilitation
Working with Partners

- Establishing the right contacts within partner agencies
- Positive diversions and Intervention Workshops
- Harnessing skills and enhancing opportunities.
Questions?

Contact Steph or Andy on cyberprevent@ersou.pnn.police.uk