REFERRALS

1 IDENTIFY

If you identify an individual you believe to be on the cusp of cyber criminality, the GMP Cyber Prevent Officer can be of help.

We aim to deter individuals from engaging in cyber offences through education and promotion of positive opportunities in the cyber industry.

2 REFER

Contact the Cyber Prevent Officer via **cyber.protectprevent@gmp.police.uk**to request the referral form. Then complete with all relevant personal information, including ability, talent, skills and capabilities in regards to cyber. Then return to the same email. Enabling the individual to be properly assessed.

3 INTERVENTION

The Cyber Prevent Officer will make contact with the referrer and confirm all details. Then make contact with the individual to deter any future involvement in cyber criminality.

4 PREVENT

An assessment will be undertaken with the individual to assess their knowledge and to enable the Cyber Prevent Officer to devise a plan. Work will be done surrounding the Computer Misuse Act, education around the consequences and promoting positive opportunities in Cyber.

RESOURCES

Cyber Security Challenge
https://cybersecuritychallenge.org.uk

Girl Geeks
http://www.girlgeeks.uk

CREST
www.crest-approved.org/

CoderDojo
https://www.comptia.org/home

Hack The Box
https://www.hackthebox.eu/individuals

Cyber Hub
https://cyberhub.org.uk/

Digital Cyber Academy
www.digitalcyberacademy.com/

GCHQ Cyber First Scheme
https://www.ncsc.gov.uk/new-talent

NCSC Cyber Aware
https://www.ncsc.gov.uk/cyberaware/home#educational-resources

Penetration Tester/Certified Ethical Hacker
https://www.eccouncil.org/

For more resources head to **www.nationalcrimeagency.gov.uk/cyber-choices** or follow the QR code

GREATER MANCHESTER POLICE

CYBER CRIME PREVENT

INFORMATION GUIDE

Cyber Prevent focuses on cyber dependent crimes, in short crimes that can only be committed by using a computer, computer network, or other form of information communications technology for example; illegal hacking, using illegal booter tools, developing malicious software i.e. malware or virus writing etc.

The aim of the cyber prevent role is to:

- **Deter individuals from getting involved in Cyber Crime**
- **Prevent individuals from delving further into Cyber Crime**
- **Reduce reoffending through education on the law surrounding online activity and the promotion of positive opportunities to legally develop skills in cyber**

Cyber Prevent also raises awareness around the Computer Misuse Act 1990 and the consequences around involvement in cyber dependent offences.

Additionally offers further information around education, training and legitimate opportunities for a career in the cyber world.

cyber.protectprevent@gmp.police.uk

COMPUTER MISUSE ACT 1990

Section 1: Unauthorised access to computer material

Example: *You watch your friend put their password in their phone, you remember the details, and without their permission you later log in and read their messages.*

Maximum penalty: 2 years in prison

Section 2: Unauthorised access with intent to commit or facilitate commission of further offences

Example: *Your friend leaves their tablet on the sofa and without their permission, you access their online shopping account and order a new computer.*

Maximum penalty: 5 years in prison

Section 3: Unauthorised acts with intent to impair, or with recklessness as to impairing, operation of a computer

Example: *You're playing an online game, but your friend scores higher than you. You use a 'Booter' to knock them offline and thereby win the game.*

Maximum penalty: 10 years in prison

Section 3A: Making, supplying or obtaining articles for use in offence under Sections 1, 3 or 3ZA

Example: *You download software so you can bypass login credentials and hack into your friends laptop, although you've not even had a chance to use it yet.*

Maximum penalty: 2 years in prison

Section 3ZA: Unauthorised acts causing, or creating risk of, serious damage

Example: *You hack into a police network. This results in delays to emergency calls, even though it was not your intention, you were reckless in your actions.*

Maximum penalty: Life Imprisonment

THE CONSEQUENCES

If you are involved in a Computer Misuse Act offence, you could end up:

- **Having all devices seized for investigation**
- **Working with the Youth Offending Service**
- **A Cyber Acceptable Behaviour Contract (ABC)**
- **A Police Caution**
- **A Serious Crime Prevention Order or Criminal Behaviour Order; where restrictions can be put on your internet and computer use, monitoring equipment installed to ensure legitimate use and interventions from the Cyber Prevent Team.**
- **A custodial prison sentence**
- **A significant fine**

Being involved in Cyber Crime can also greatly reduce your job prospects and further career aspirations. Some companies will not hire individuals with criminal convictions and under the Rehabilitation of Offenders Act, offences have to be declared for a set period of time.

In addition entry to other countries can be prohibited. VISA's for places like the USA and Australia can be denied.

Criminal convictions can also have a detrimental affect on your housing choices and eligibility to borrow money as this information is often revealed during background checks.

SPOTTING THE SIGNS

The average age of someone arrested for a cyber crime offence is 17 years old.

The world of cyber can be very enticing, especially to young people. Many individuals may do things online, not realising they are breaking the law.

If you think someone you know may be on the cusp of cyber crime involvement, here's a few signs to look out for:

- **Become withdrawn and spend large amounts of time locked away on their computer**
- **They may have no real friends but talk to many people online**
- **They may use very technical language or hacking terminology such as 'DdoS, Black Hats, Botnets, Keylogger etc**
- **May have multiple email addresses and social media accounts**
- **Poor sleeping/eating habits due to excess online activity**
- **Claim to be making money from computer games**
- **Have lots of money but no source of legitimate income**
- **May refer to themselves as a hacker or script kiddie**
- **They may talk about the deep web or dark net**
- **Internet use could be slow around them as other hackers try to overload them**

If you notice any of the above behaviour please feel free to contact Cyber Protect and Prevent for support and advice.