A Career With Great Results Or Serious Consequences - 01.03.20

Cybercrime is a major and growing problem, targeting people, companies and even government organisations, causing financial and identity fraud, data theft and serious disruption. Some cybercrimes are carried out by individuals, others by organised crime groups. Like legitimate companies, these groups all have managers, employees and subcontractors who have all been drawn in, one way or another.

What does this have to do with your child?

Some of the most serious cybercrimes are either committed or aided by children as young as 12. Typically, they're super-talented at IT and often spend many hours on their computer in their bedroom. They may have been attracted via gaming, coding or hacking forums, also populated by cybercriminals. Their parents are usually unaware … just happy that they're learning, keeping themselves occupied and not getting into mischief on the street.

Several of the people jailed for the hack on telecoms business TalkTalk were teenagers at the time of the attack in October 2015. A hacker for hire who crossed the line into cybercrime at just 13, was sentenced for breaking into global institutions … from his bedroom. It's thought that as many as one in four UK teenagers have tried some form of internet hacking.

Unchecked, they could be money laundering for organised crime groups, writing or distributing malware, breaking into innocent people's bank accounts or hacking official websites. For many, it's a way to make serious money. For others, it's a way to gain the respect of their peers, or just for the excitement. Some don't even realise they're doing anything wrong.

These are all somebody's children. Could they be yours?

Cybercrime is not a victimless crime, and the National Crime Agency (NCA) and police take it very seriously. They work with national and international partners to investigate cybercriminals of all ages. Children who get involved could face the following consequences:

- A visit and warning from Police or NCA officers
- Being arrested
- Having their (or your) computer seized and internet access restricted
- Paying a penalty or fine
- A significant prison sentence
- A permanent criminal record, which could affect your child's education, future career prospects and ability to travel abroad.

What you should do?

If your child has an interest in computers/technology, it's important to have a discussion with them about their use of it. Recognising and engaging with this interest is key to ensuring that they follow the correct pathway. Below, we've listed some tools which can indicate a child's interest in technology, but can be used for both legal and illegal purposes. If you see one or more of these tools on your child's device, it's worth talking about them.

- TOR – the most commonplace browser used to access the dark web
- Virtual machines – enable a user to run multiple, different operating systems on one computer
- Metasploit – a free kit of tools used by both illegal and legitimate cybercriminals for hacking, exploits and malware distribution
- Kali Linux – designed as a legal tool for testing and forensics, it features over 600 tools which are also used by illicit hackers
- Pineapple – a compact device with antennae that plugs into a computer to capture communications between devices and unsecured Wi-Fi networks.

If you're concerned, talk with your child about the importance of honesty and legality, the consequences of involvement with cybercrime and the highly satisfying, lucrative and legal options available to them, such as coding, engineering, development, testing, security operations, detection, law enforcement, legal hacking, and many more roles in both the public and private sectors.

Search for computing and coding clubs available in your area and encourage your child to join the appropriate one for their age and ability.

If you're concerned or would like advice on how to guide your child down the right path, please don't hesitate to email cyberchoices@nca.gov.uk. In most cases, the NCA or one of their regional partners will provide you with expert advice and be happy to talk to your child before things go too far.

Get Safe Online

Get Safe Online is the UK's leading source of information and advice on online safety and security, for the public and small businesses. It is a not-for-profit, public/private sector partnership backed by a number of government departments, law enforcement agencies and leading organisations in internet security, banking and retail.

For more information and expert, easy-to-follow, impartial advice on safeguarding yourself, your family, finances, devices and workplace, visit www.getsafeonline.org.

If you think you have been a victim of fraud, report it to Action Fraud at http://actionfraud.police.uk or by calling 0300 123 2040. If you are in Scotland, contact Police Scotland on 101.