CYBER CRIME VS CYBER SECURITY: WHAT WILL YOU CHOOSE?

Public awareness and prevention

Download the poster in different languages.

DOWNLOAD THE POSTER IN VARIOUS LANGUAGES

It is not unusual for teenagers and young people to get involved in cybercriminal activities at an early age. Some do it for fun without realising the consequences of their actions – but the penalties can be severe. Cybercrime isn't a victimless crime and it is taken extremely seriously by law enforcement. The minors that become involved in cybercrime often have a skill set that could be put to a positive use. Skills in coding, gaming, computer programming, cyber security or anything IT-related are in high demand and there are many professional careers and opportunities available to anyone with IT talent and an interest in these areas.

WHAT ARE SOME EXAMPLES OF CYBERCRIMES THAT INVOLVE PREDOMINANTLY YOUNG OFFENDERS?

- Hacking – involves gaining access to someone's computer network without their permission and then taking control, and/or taking information from an organisation, agency or individual. Basic examples may include accessing a secure area on a school's computer network to look for test paper answers or trying to change test scores.
- Malicious software - making, supplying, or obtaining malware, viruses, spyware, botnets, and Remote Access Trojans (RATs) is a criminal activity. These programmes allow cybercriminals to get into other people's computers without their permission. "Pranking", by remotely accessing a friend's computer without their knowledge and messing around with it, is illegal.
- DDoS - a Distributed Denial of Service (DDoS) attack, or 'booting', consists of sending a large amount of internet traffic towards a website to stop somebody or anybody from accessing it. Booting someone offline whilst playing online games may seem like a harmless joke, it may be challenging and entertaining - but it is illegal.

- In most countries, if someone is caught doing something even as simple as using a stresser to boot another player out of an online game, he/she could get under the radar of the police and, if they keep doing it, even a prison sentence.
- Less tech-savvy youngsters, also known as 'script kiddies', could use stressers to attack a website they dislike, or even their school's website. They are often unaware that this is illegal and see it as a simple prank. However, it is a criminal activity and the consequences can be serious!
- Becoming involved with DDoS attacks is considered a gateway crime, leading to more serious activities, including ransomware attacks. Even though the youngsters involved do not pursue this activity for the financial rewards, they could become entangled in various illegal activities and even organized crime groups.

WHAT CAN GO WRONG?

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

Consequences vary from country to country, but young people who get involved in cybercrime could face the following:

- A visit and a warning from the police, as well as a penalty fine
- Arrest and a prison sentence for serious offences
- Their computers being seized and/or being prevented from accessing the internet

ADVICE FOR TEACHERS

- TALK - If you are worried about one of your students, speak to them about what they are doing, try and point out the difference between harmless exploration/curiosity online and illegal online activity. Tell them about the consequences of cybercrime for the offender and for the victim. Try mentoring them and showing them positive ways to use their skills. If you are very concerned, you should consider alerting the students' parents.
- DETER- The best way to help to deter tech-savvy and talented students from getting involved in entry level cybercrimes is to offer them constructive and positive alternatives. Check out the resources below.

REPORT - If you believe that your school is the victim of a cybercrime attack or that a student is engaging in cybercriminal activities, you should report it to the school and to the local police: Report Cybercrime Online

ADVICE FOR PARENTS

Given the past years' fast technological progress, is it quite common for children to easily become tech-savvy. However, they still need your help and guidance to make sure that they stay on the right path. Unfortunately, their talent could be exploited by cybercriminals rather than put to good use in the world of cybersecurity. Once they are on the radar of law enforcement, their professional and educational futures might be compromised. Cybersecurity companies tend to avoid hiring convicted hackers, regardless of how talented and tech-savvy they might be.

WARNING SIGNS

Some of the indicators that your child may be at risk of becoming involved in cybercrime include:

- They spend most of their time online and are often secretive about their activities;
- They are excessively interested in coding;
- They seem to gain an additional income from their online activities, but they do not talk about how they do it;
- Your home network's monthly data allowance is often met;
- They socialize more in the online world than offline

Many children will have an active interest in coding and programming, spend a lot of time online and have independent learning materials. These are all signs of a healthy and positive interest in computing and the development of those extremely valuable skills should be encouraged – but in a lawful way.

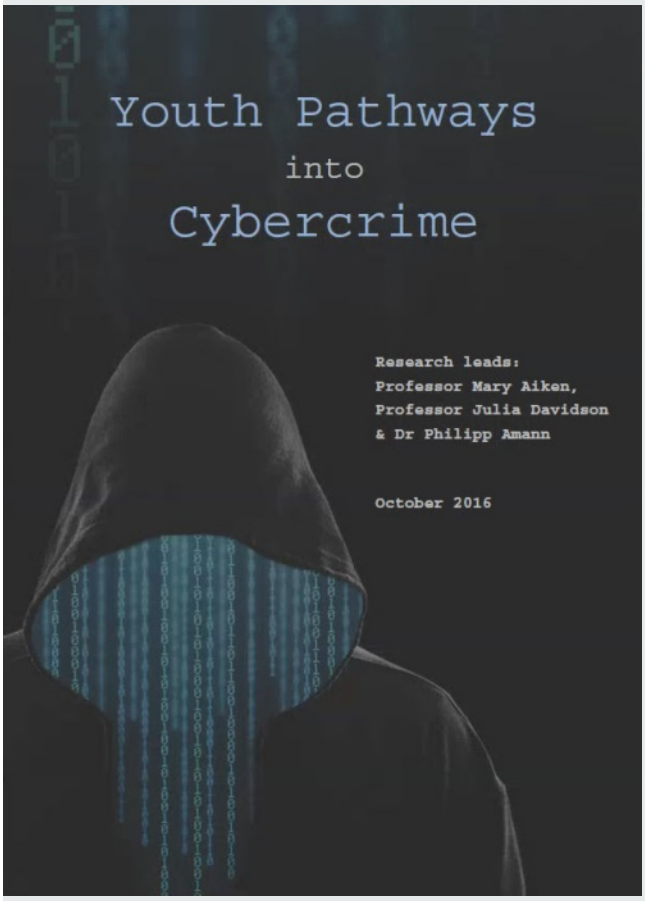
The research paper “Youth Pathways into Cybercrime” attempts to explain the pathways that lead some young people into cybercrime. The report highlights the need to develop effective prevention and intervention strategies as well as the importance of promoting alternatives, positive (and legal) ways of channelling young talents toward careers in the tech and security sectors.

Youth Pathways into Cybercrime: case study

Teenage hacking of online forum

Luke, a teenage boy, is thrilled by the challenge of hacking into websites. He starts learning hacking skills by asking questions on forums and experimenting with freely available hacking tools. Luke learns about Hydra, a network logon cracker program that automatically tries username and password combinations from a large list of known usernames and passwords to “lockpick” access to the target website. Hydra frequently succeeds, because users tend to choose simple passwords and reuse them on different websites. Luke starts using Hydra to hack into web forums.
At first he uses a list of usernames and passwords publicly available on the Internet, but once he succeeds in getting administrator access to a forum, he expands his list with the contents of the compromised forum database, which makes Luke more effective at hacking other online forums.
Although Luke’s technical skills are not very advanced, the combination of freely available hacking tools, tutorials and advice from other hackers allowed Luke to be an effective hacker for a time. His hacking is eventually discovered by the administrator of a popular online forum and Luke is apprehended by the police.

Download the research Youth Pathways into Cybercrime.



WHAT CAN YOU DO?

- TALK – chat with your child/teenager about acceptable online behaviour. Take an interest in what they do, help them understand the difference between right and wrong in the cyber world, just as you would do in any offline world situation
- BEHAVIOUR - talk to them about ethical behaviour online. Some real life rules apply in the online world too. The following types of behaviour are to be avoided:

Stealing or using anything online that is not free or doesn't belong to them.

Harming anyone – while it might not be as obvious as in the real world, cybercrime is not victimless.

Bullying anyone, through chat, social media or any other online means.

Being disrespectful or impolite online – they should not use their digital knowledge to hurt others.

Hacking - using RATs, DDoS attacks, stressers/booters to attack others is not just unethical, but illegal.

Remember - your children might not be aware that their actions could lead to a criminal conviction. In spite of what their friends tell them, law enforcement is always going to catch up with illegal online activity and identify the perpetrators. Europol's European Cybercrime Centre is often coordinating operations involving such targets. Operation TarPit and Operation Neuland are two examples of such operations.

- LISTEN - try to learn about and understand how they spend their time online. Try to assess their level of cyber knowledge and offer them alternatives. If your child is passionate about computing, make sure you look into opportunities to further their education. For more on this, see our list of resources below.

POSITIVE ALTERNATIVE RESOURCES AT EU LEVEL:

European Cyber Security Challenge

- The participating EU Member States organize annual national cyber security competitions open to young people between the ages of 14 and 25. The best players from each of these national competitions then go on to reach the EU-wide final European Cyber Security Challenge (ECSC). The ECSC is hosted by a different country each year and involves a set of challenges: capture the flag, jeopardy, attack-defence, etc. The event is accompanied by a

cyber security conference and/or a job fair.

European Cyber Security Month

- EU's annual advocacy campaign that takes place in October and aims to raise awareness of cybersecurity threats, promote cybersecurity among citizens, and provide up to date security information through education and the sharing of good practices. Hundreds of cyber-related activities are organised throughout Europe every year during this month

European Code Week

- A grass-roots movement that celebrates creating with code. The idea is to make programming more visible and show young people, adults, and the elderly how to bring ideas to life with code, to demystify these skills and bring motivated people together to learn. The initiative was launched in 2013 by the Young Advisors for the Digital Agenda Europe. The website also includes a comprehensive list of resources and guides related to coding, in various languages and targeted at both beginners and advanced learners.

Digital Skills and Jobs Coalition pledges:

- The Digital Skills and Jobs Coalition brings together Member States, companies, social partners, non-profit organisations, and education providers who take action to tackle the lack of digital skills in Europe. The Coalition addresses the need for digital skills at all levels, including ensuring better digital skills training for youngsters. Find out more about the Coalition here .
    - The initiative encourages all organizations, businesses and government bodies to make a concrete commitment to carry out actions to reduce the digital skills gap in Europe. These commitments, or pledges, range from teacher training, reskilling jobseekers and actions targeting ICT professionals to resources for tech-savvy young people. You can find all the pledges in the pledge viewer .

International Cyber Security Summer School

- The International Cyber Security Summer School allows students and young professionals to gain deeper knowledge and understanding of cyber security concepts, as they learn about the latest cybercrime threats and trends as well as the cutting edge cyber security features that exist today.

LEGAL DISCLAIMER

Legal Disclaimer - Cyber Crime vs Cyber Security: What Will You Choose?

The information and advice published on this page is offered for general purposes only, free of charge, on an "as is" basis, without being tailored to individual situations and should not be considered as professional advice. The decision on whether to participate in a presented project or event is taken at your own risk. Europol bears no responsibility for those projects or events which are organised by third parties.

This page contains links to other websites developed, controlled and maintained by third parties. Europol is not responsible for their content and the applicable policies. By clicking on a link and navigating outside Europol's own website, you may need to agree to third parties terms and conditions and may be subject to their policies.

The inclusion of external links on this page does not imply Europol's endorsement of any participating entity. Europol provides links to non-commercial webpages and these are checked prior to their posting on this page, however please keep in mind that these checks are limited and that pages may be altered. It is also possible that with a few clicks you will navigate to pages offering commercial services. Europol is not linked and does not endorse such commercial activities and the entities providing them.

With the exception of Europol logo (for which specific authorisation is required), the information on this page may be reproduced without further Europol authorisation in any format or medium provided that the source is identified and the copyright status acknowledged. Information and/or material may not be used as to imply in any way that Europol endorses a product, service or action.

To our reasonable knowledge, the information and the materials published on this page are legal, decent and truthful, comply with laws and regulations and do not infringe the Intellectual property rights of any third party.

The main language of this page and of the material is English, which should be considered as original and should prevail over other versions. To our knowledge, translations are made faithfully and the original content is not modified in any way, with exception of minor language (dialect) issues. We decline any liability for any omissions and/or errors in the translated version of the material.

If you have any questions with respect to the project, please contact us.

CRIME AREAS	Cybercrime
TARGET GROUPS	General Public • Law Enforcement • Academia • Professor • Students • Researcher • Press/Journalists • Other
GENERAL TERMS	Campaign • Public Awareness & Prevention
ENTITIES	European Cybercrime Center (EC3)