Research Highlights for
Children's Online Safety
#101
November, 2016

UK COUNCIL FOR CHILD INTERNET SAFETY

CATS

Youth Pathways into Cybercrime

Aims

This Research Highlights presents the findings from a study exploring youth pathways into cybercrime. As an upwards trend in cyber-victimisation becomes increasingly apparent, and more young people are engaging with technology in new and different ways, there is a real need to understand the pathways into cyber-criminality from a range of perspectives. This project engaged with a range of stakeholders to highlight how those dealing with anti-social and criminal youth online are seeing the trajectories emerge and progress. It also intended to inform policy, industry and police practice in the realm of youth hacking. This can inform professional practice within key infrastructures under threat of cyber-attacks; influence educational awareness in homes and schools; and focus on vulnerable yet able young people who may not be fully aware of the dangers and severity of online deviance.

Key Findings

The analysis identified particular characteristics and features of adolescent hackers in contemporary society, whilst also providing key recommendations illustrating important considerations for policy, policing and cyber-security:

- Integrating elements of **criminology, cyberpsychology, neurobiology** and **developmental psychology** is necessary to have a holistic understanding of pathways into cybercrime.
- Key demographic features include a large proportion of **adolescents** with **high IQ's** and **high computer literacy**. They come from a **broad** range of social classes and are often **socially isolated** from mainstream peer groups. They may also be socially **awkward** and **withdrawn**.
- This group of young people also demonstrate:
    - High need for online **affiliation** and **affirmation** in improving their **online reputations** which may compensate for their lack of real world **self-esteem**.
    - Willingness to engage in **low** level illegal activity online, which may **escalate** through positive **reinforcement** of easily accessibly rewards and online peer groups.
    - Behaviour as a consequence of normalisation, positive reinforcement and reputation may become **addictive**.

A series of recommendations were made in dealing with young people moving forward:

- Society must focus on **awareness raising** informing youth and parents of the consequences of engaging in online illegal activity.
- **Education** must take a central role in prevention and intervention.
- Improve the ability of communities to **identify** those most at risk.
- Support **practitioners** working with young people.
- Developing appropriate **cyber 'role models'** including **peer-mentoring** is critical in illustrating the positive side of their abilities to young people.
- The implementation of a **Technology Quotient (T.Q.)** to be utilised in conjunction with measures of I.Q., E.Q. and C.Q. may assist in moving towards a more holistic understanding of young people and technology.

Research Highlights for Children's Online Safety #101
November, 2016

UK COUNCIL FOR CHILD INTERNET SAFETY

CATS

Policy Context

Financial cybercrime is a global phenomenon in which billions of pounds are lost each year. It is essential that governmental institutions recognise the level of criminality occurring. Increasingly, stories of highly able youth exploring the cyber landscape and finding themselves in serious trouble are reported in the media. It is imperative that comprehensive policies focusing upon deterrence, prevention and rehabilitation are developed that consider potential loss to industry, but also consider the needs of often vulnerable young perpetrators, as well as victim protection.

Methodology

The methodology was divided into two primary phases: literature review and scoping; and a series of stakeholder interviews. The literature review focused on bringing together seminal as well as innovative research exploring cybercrime from 5 key perspectives: developmental psychology; neurobiology; criminology; computer science; and cyber-psychology. Key pieces of policy and legislation surrounding cybercrime, as well as text books and high impact peer-review journals, were consulted in bringing together the literature based evidence. This resulted in the inclusion of over 100 pieces of distinct research. The second phase, that of the stakeholder interviews, involved 10 participants from a range of sectors: education, law enforcement, and computer sciences. This explored understanding of youth pathways into cybercrime, whilst discussing where resources and attention needs to be placed. The interviews were transcribed and analysed for themes linked to the overall question of understanding how these youth are being drawn into crime, and what we can do about it moving forward.

Background

Online activities and behaviours can be complicated to measure and difficult to understand due to their novel nature and manifestations. In particular, children and adolescents who are growing up completely immersed in the virtual world are 'digital natives', providing society with a new and ever evolving cohort of developing individuals who are being influenced by technology. More specifically, these young people are being attracted and drawn into anti-social behaviour and deviance in the online sphere in increasing numbers. This is a global issue which has a myriad of economic, developmental and societal implications. As these crimes evolve in frequency, modus operandi and consequences, more work needs to be done in terms of prevention, education and intervention, particularly with this vulnerable and able group of youth. This research project was undertaken as there is an urgent need to understand the pathways that lead some young people into cybercrime.

Source Youth Pathways into Cybercrime: Final Report 2016 (October 2016).
Available at: http://www.mdx.ac.uk/__data/assets/pdf_file/0025/245554/Pathways-White-Paper.pdf

Research Team Professor Julia Davidson (PI), Professor Mary Aiken (PI) & Dr. Phillip Amman (PI); Dr. Jeffrey DeMarco (Project Manager)

Contact information Dr. Jeffrey DeMarco, Centre for Abuse and Trauma Studies (j.demarco@mdx.ac.uk)

RH#101 has been produced by Dr. Jeffrey DeMarco for the UKCCIS Evidence Group