OpenLearn

The Open University

The psychology of cybercrime

This item contains selected online content. It is for use alongside, not as a replacement for the module website, which is the primary study format and contains activities and resources that cannot be replicated in the printed versions.

About this free course

This free course is an adapted extract from DD802 *Investigating forensic psychology.*.

This version of the content may include video, images and interactive content that may not be optimised for your device.

You can experience this free course as it was originally designed on OpenLearn, the home of free learning from The Open University – https://www.open.edu/openlearn/health-sports-psychology/psychology/the-psychology-cybercrime/content-section-0

There you'll also be able to track your progress via your activity record, which you can use to demonstrate your learning.

Contents

Introduction

In this free course, *The psychology of cybercrime*, you will explore different questions about cybercrime from a psychological angle in an attempt to better understand this relatively recent field of psychology. You will consider the realms and limits of cybercrime, distinguishing between the different types of cybercrime (e.g. trolling, cyber-stalking, fraud, hacking), the experiences of being victims of cybercrime and the causes behind engaging in these types of criminal activity. Finally, current interventions will be highlighted.

Even though cybercrime is broadly encompassing all the different types of crime committed online, it is important to emphasise very early on that it is likely to be committed by offenders with different characteristics, motivations and behaviours than those who commit other types of crime. As a result, those online criminal activities share similarities with offline equivalents (e.g. fraud and online fraud). The interest in studying the psychology of cybercrime both from the perpetrator and victim perspectives has arisen in an attempt to understand what makes cybercrime unique or similar to its offline counterpart.

Content warning

Cybercrime victimisation can affect both adults and children who engage online. Please find links to two useful guides that give tips on to stay safe online:

1. Cybercrime and online safety developed by West Yorkshire police.
2. Supporting your child's wellbeing by the NSPCC.

This Open Learn course is an adapted extract from the Open University course DD802 *Investigating forensic psychology.* Explore the collection of Postgraduate study in psychology and criminology.

Learning Outcomes

After studying this course you should be able to:

- outline the impact on victims
- distinguish different types of cybercrime, considering the similarities and differences in the definitions and behaviours
- identify the motivations and behaviours of cybercriminals
- illustrate the current interventions to tackle cybercrime.

1 What is cybercrime?

Cybercrime refers to criminal activities that are committed using internet technology. The internet has only been in widespread use by the general public for a few decades (a ‘start date’ could be considered to be the launch of the World Wide Web on the 6 August 1991), but online activity has already become ubiquitous in the developed world and is becoming progressively more common in much of the developing world as well (Naughton, 2016).

Psychologists studying cybercrime, including its perpetrators and victims, are interested both in what makes cybercrime unique (e.g. does online anonymity increase the propensity of some people to commit crimes of harassment?) as well as what it has in common with offline crime – although the emphasis is often on the former rather than the latter.

Before reading further complete Activity 1. In order to help you complete the activity, please watch the following video and then consider your perspectives on living online.

Video content is not available in this format.

Video 1 Everyday perspectives: engaging online

Activity 1 Thinking about cybercrime

Allow 20 minutes

Try to answer the following questions about cybercrime, drawing on your experiences and understandings. Type your responses (up to 100 words for each question) in the box below, and then select ‘Save’. Your responses are not published anywhere.

1. Think about how you engage online. Make a list of the things you do online (e.g. social contact, looking for information, news, weather, sports, entertainment, studying online, shopping, bank, holiday booking and so on)

Provide your answer...

2. Looking at your answers above, try to guess how much time you spend on a weekly basis on each activity and your potential victimisation

Provide your answer...

Discussion

According to Ofcom (2020), 87% of UK adults spent an average of 25 hours online per week. People go online for the following reasons (How People use the internet, 2020):

- social networks (including video calling)
- email
- be entertained (watching videos, music, online radio and podcasts)
- get information (search, blogs)
- news (including online newspapers, magazines)
- online games
- banking
- work (either earning money online or using the internet to work remotely)
- shopping
- education
- other access.

You might have put online fraud (such as issues around scams and various security breaches when paying or banking online. You might have thought about more subtle forms of victimisations such as trolling or cyberbullying on social media for instance or issues around protection of identity and reputation.

As already indicated in the content warning in the introduction, you can download a comprehensive guide on cybercrime and online safety developed by West Yorkshire police in order to get tips about how to increase your online safety. Alternatively, the NSPCC has developed a range of resources regarding child safety online. More guidance about online safety regarding specific online activities will be provided towards the end of the course.

2 Types of cybercrime

As you have probably identified from engaging in Activity 1, the internet offers a wide range of activities and opportunities for criminals to engage in anti-social and/or deviant behaviours. Therefore, the term cybercrime encompasses a variety of different activities, which goes beyond the fact that they are either a function of, or are facilitated by, the internet. Indeed, real-world crimes can be seen to achieve different goals; for example, theft for financial gain compared to murder for the purpose of revenge. In the same respect, criminal activities falling under the umbrella of cybercrime follow the same pattern. Usually, a distinction is made between:

i. **instrumental crimes** (i.e. crimes where the harm to the victim is not the ultimate aim) and
ii. **expressive crimes** (i.e. crimes are based on an offender's emotional response to a situation that provokes anger, leading to a desire to cause harm to the victim) (Canter and Youngs, 2009; Youngs, Ioannou and Eagles, 2016).

Similarly in an online environment, some forms of crime seem to principally be for financial gain (e.g. **ransomware** attacks, online identity theft), whereas others may be carried out for personal reasons, such as revenge (e.g. cyberstalking) or for the purposes of furthering an offline crime (e.g. a paedophile grooming a child online). However, there are also offences/anti-social online behaviours such as 'hacking' and 'trolling', which may be carried out for a variety of other reasons.

Activity 2 Classifying the different types of cybercrime

Allow 20 minutes

Many categorisations of cybercrime distinguish between crimes against the person/ morality and crimes again property/government. Use your common knowledge to decide whether this falls under crimes against the person or crime against the property or both. Put some text into the boxes you think are the right option.

Table 1 Classifying the different types of cybercrime

	Crime against the person	Crime against the property	Both	
Malware				
Trojan				
Virus				
Worm				
Ransomware				
Phishing				

Online financial crimes				
Online Fraud				
Password cracking				
Hacking				
Photo-hacking				
Sextortion				
Image-based sexual crimes				
Revenge Pornography				
Cyberstalking				
Trolling				
Cyberbullying				

Discussion

Under that assumption, cyberbullying, trolling and cyberstalking, revenge pornography, image-based sexual crimes, sextortion, photo-hacking, hacking are likely to fall under the crime against the person category. Malware (including trojan, virus, worm), online financial crimes (including online fraud and password cracking) are more likely to fall under the crimes against the property category. However, you have probably realised that for many crimes it is not as clear cut and could be both directed at the person and the property (even if one is a by-product of obtaining the desired object or status) such as image-based sexual crimes who at face value could be seen as a crime against property (i.e. stealing an image) but ultimately it is a crime against the person. Moreover, cybercriminals usually combine criminal behaviours such as cyberstalking, sextortion, revenge pornography and possibly cyberbullying, therefore people can easily be victim of two (or more) types of cybercrimes simultaneously. Now have a look at some of them in details in the next sections.

2.1 Trolling

The term trolling has been widely used since the apparition of the internet and it refers to all online deviant behaviours generated by individuals towards other individuals and/or

groups that are repetitive and disruptive in nature (Fichman & Sanfilippo, 2016). However, this is slightly simplistic as trolling behaviours do evolve constantly in line with how the online environment itself changes. Vaisman and Fichman (2012), cited in Fichman & Sanfilippo, (2016, p.6) consider four factors to explain the variety within trolling behaviours depending on:

i. *Location*: The distinction between asynchronous (when people communicate but not at the same time such as blog comments) and synchronous communication (live conversation such as chat room). Both types of trolling exist but it is more difficult to account for within synchronous settings as the context is not recorded (Fichman & Sanfilippo, 2016).

ii. *Relationships*: Trolls usually target random, innocent people as well as the community. When they start targeting individuals, it overlaps with other online deviant behaviours such as harassment or bullying. According to Fichman and Sanfilippo (2016), trolls usually act individually and usually hide their identity, though they can coordinate their behaviours with other trolls as there are evidence of camaraderie between trolls such as in the controversial online platform TATTLE.life where people gather to openly and freely troll about social media influencers, even referring themselves as trolls (e.g. tattle trolls….), or reflecting on what is an online troll? – See #tattlelife. The reasons why this website has received so much attention is that the purpose of the site is to group people with trolling tendencies together. Therefore, group trolling not only normalises this type of behaviour but also it intensifies the damage under the greatest anonymity with made up usernames (Fogarty, 2019).

iii. *Intentions*: Originally trolling behaviours were thought as being unintentional because it was just for fun (Buckels, Trapnell, & Paulhus, 2014). While you could find up to 135 different types of trolls identified from many online resources (Nuccitelli, n. d.), psychological evidence has been more reserved in categorising the different types of online trolls. Indeed, research has mostly focused on motivations or intentions either looking at personality (e.g., Buckels et al., 2014), or explanations of intentions such as being ideological, non-ideological, religion driven, grief driven, fun driven, or political (Fichman & Sanfilippo, 2016). However, as Coles and West (2016) argued, beyond the broadness of the term ‘troll’ and the many subtypes, it is important to look at the term as having variable meanings, intentions, and varied sub-types between different platforms and the course of interaction.

iv. *Behavioural practices*: Trolls themselves usually do not identify their behaviour as being aggressive but more as being opiniated. However, the pattern is that trolls usually set ‘discursive’ trap to create a reaction through controversial comments or questions. What truly defines someone as a troll is the repetitive action of their behaviour towards the same individual or online community, repeating the same ideas and ignoring the responses and challenges directed at them (Shachaf & Hara, 2010).

Activity 3 Which of these examples is trolling?

Allow 10 minutes

Jane Doe posted the following on a popular social media site.

Jane Doe
@Jane_Doe

Following

I believe in Science. And empirical evidence.

05.34 · 22/07/2020

Look at the six examples of trolling below and decide whether you feel it falls under the trolling category or being opiniated. Type your anwer into the box.

Table 2 Replying to @Jane_Doe:

'… and very poor grammar