Public Thoughts on Tackling Digital Crime in Society and by Law Enforcement

G. Humphries

Computing, Digital Forensics and Cybersecurity, Canterbury Christ Church University, Canterbury, United Kingdom
e-mail: georgina.humphries@canterbury.ac.uk

Abstract

With the ownership of connected digital devices standing at 3 for the average user, the ubiquity of the Internet and the rise in smarter Internet-connected devices, there is an inevitable increase in the rise of digital crime associated with such devices. Well-known is the under-reporting of cybercriminal activities by victims which may give a green light for continued online criminal activities. Yet, there is little focus on the wider public's perception on what needs to be tackled in relation to digital and online crimes; this paper examines and discusses the views of 102 questionnaire responses from public participants. Questions and responses focused on societal challenges surrounding digital technologies and the perception of law enforcement's role in digital and online crimes. Crimes described or listed by participants are coded into themes addressing participant concerns surrounding digital crime. This study also discusses those participants who identified as 'victims of digital crime' (n=25) and offers them to share the actions they took as well as any outcomes. This study found nearly a quarter of respondents have been a victim of dishonest or unlawful behaviour online. This paper speculates how some criminal activities may be under-reported due to lack of awareness alongside the underappreciation for the extent and spread of such crimes. Results show that participants were heavily focused on crimes such as, theft, fraud and those involving children.

Keywords

Cyber Security, Digital Forensics, Cyber Crime, Human Behaviour, Public Perception

1 Introduction

With the growth of Internet-connected devices and number of Internet users over the past 10 years rising year on year (Murphy and Roser, 2019), several questions may be posed surrounding the security of data online and the number of digital and online crimes which take place. Until recently, in the UK there was no single household crime survey which considered online crimes. The National Crime Agency (2016) notes that "[u]nder-reporting [of cyber crime] continues to obscure the impact of cyber crime on the UK". In more recent years, the Crime Survey for England and Wales (CSEW) includes computer-based crimes looking to identify under-reporting of, for example, computer misuse and fraud.

The Office for National Statistics (2018b) classified approximately 4.7 million fraud and computer misuse incidents; where approximately "1.8 million [fraud] incidents" were cyber-related ending September 2017. Over 900,000 (64%) of incidents were related to computer viruses and over 540,000 incidents (36%) were associated with unauthorised access to personal information which included incidents of hacking (The Office for National Statistics, 2018a). Furthermore, the highest proportion of loss due to fraud was associated with "Bank and credit account fraud", accounting for nearly "2.4 million incidents" with over 2 million victims (The Office for National Statistics, 2018b). More recent statistics show that there has been a decrease in the number incidents involving misuse and viruses in the period 2017 to 2018, however, the survey continues to point to over a million computer misuse offences (The Office for National Statistics, 2019). This is a statistic which substantially differs from those reported by other organisations in the same year (The Office for National Statistics, 2019).

This paper extends from the idea of capturing the views of public participants on the meaning and understanding of cyber security and digital forensics. The aim is to identify and analyse what the wider populace feel should be tackled in society and what law enforcement should focus on in relation to digital and online/cyber-related crimes.

2 Method

Responses were collected from 102 participants using an online questionnaire which was distributed across messaging and social media platforms known to the researcher. Convenience sampling was used for ease of access to a wider audience; however, inferences from these results can only be made about the sample collected. Google Forms was used as the survey platform to design questions which were both open and closed. This ensured the public's perceptions were captured and reduced researcher bias. A pilot test was conducted on a small group of reviewers allowing the researcher to check study feasibility, data collection process, measurement instruments as well as the meaningfulness of data for analysis before final delivery. The foci and motivation of the questionnaire centres on discovering the perceptions, views, experiences and understanding of cyber security and digital forensics of several target audiences, one audience being the public. In particular, the identification of what they believe should be tackled in society and by law enforcement. 102 participants took part in this study, of which 59 identified as female and 38 as male. 72 respondents documented they were in full-time employment, 7 in part-time employment, 7 self-employed, 10 were retired, 3 were students, 2 were unemployed and 1 stated "other". The highest qualification held by most respondents was a Bachelor's Degree (30), followed by an A-Level or equivalent (18), then a Master's Degree and GCSE level/equivalent (13 respectively). 52 of the participants were aged 41 and over.

Part of this survey was previously used to identify the public's views on cyber security, digital forensics and their use of digital devices. Additionally, this survey collected responses from individuals on their views for what needs to be tackled in society and by the police to confront digital and online crime as well as if they had ever been a victim of such crime. Responses collected were examined and open coded into themes which draw on several crimes, aspects of societal change and the need for awareness which participants feel are important.

3 Results and Discussion

Results below are based on the views of 102 participants who were asked two questions on how digital crime can be tackled in society and by law enforcement:

- What do you feel needs to be tackled in society in relation to digital crime and cyber security?
- What online or cybercrime do you want and expect police officers to be tackling?

While also discovering if any participants had fallen victim of such crimes, as well as their responses and any outcomes. Arguably, the openness of the abovementioned questions may allow for vague interpretation and condense several sub-questions, however, the broad and open-ended approach allowed for a richness in response which could not be obtained through closed questions. Accepting a range of responses based on the participants own understanding, views and perceptions of various issues relating to digital and cyber crimes. Thus, providing the researcher with the chance to analyse, code and categorise responses.

3.1 Victimisation: participants who fell victim to digital and online crime

Of the 102 individuals, 25 recognised having been a victim of a digital/cyber-related crime, 1 of minor crime (spam), plus 1 who stated: “almost when a guy called for the other half of my online banking details”. This left 75 individuals responding saying they had not been a victim of such crime. With nearly 25% having been a victim of digital crime, further analysis into how the victims responded and the people’s views on what needs to be tackled were obtained.

Examples of criminal activities included a range of account hacks (including bank and social media), online harassment and threats. Of those who fell victim, 60% were that of bank card/online banking fraud, followed by phishing attacks (32%) and online fraud of goods (e.g., goods purchased but not delivered/counterfeit) (28%). A similar trait to aforementioned statistics introduced in this study, a high proportion of respondents associated acts of fraud to online banking activities demonstrating there is still much progress to be made when it comes to online activities and security, both technical and human aspects.

Participants were asked how they responded to these crimes; for example, did they report the crime and what was the outcome? Responses included contacting relevant banks and email service providers to investigate and fix the incident. Respondents noted little damage or loss often due to the “quick thinking of [their] bank” or money was “refunded” and any “black marks … erased”. A few respondents recognised how the crime they suffered was due to insider efforts where employees were sacked, or websites were closed, and arrests made.

Other participants expressed their interest in responding through learning how to defend themselves; one characterises their response with efforts placed in “becom[ing] a keyboard warrior & learn[ing] basic digital self defense/preservation". However, the term 'keyboard warrior' is coined as an informal noun to mean someone who displays aggressive tendencies and posts in an online setting, while concealing their real identity (Cambridge University Press, 2013). It is understood that this is not what the respondent implies, and that they are in fact vocalising their own needs, as well as others, to become more skilled to defend themselves and implement security mechanisms on devices, adding caution online. Another stated how they "step[ped] up all online passwords using random strings saved using external software installed on [their] computers and smart devices (the latter of which requires fingerprint authorization)". In some cases, individuals are educating themselves in ways to prevent becoming a victim by using stronger security measures. This shows a change in behaviour, initiative and awareness: all human factors relating to digital crime and prevention.

Results show that 17 victims reported the crime to the relevant authorities, some resulting in the identification of criminals and leading to arrests, while others were fully reimbursed, and all issues resolved. This left nine individuals (approx. 35%) who did not report the crime, supporting the belief that there are greater possibilities and costs associated to digital crimes due to unknown and under-reported crimes.

It was not uncommon for respondents in this survey to fall victim to multiple crimes. Participants often classified crimes as several incidents, with four incidents of hacking, six as having discovered malicious software, eight as phishing and seven as online retail fraud. This study found a greater percentage of respondents reported the crime to relevant authorities demonstrating an awareness among this sample and the need for a reactive approach. Curiosity here surrounds whether people realise they have been attacked in similar circumstances across all generations; a wider study is required to discover this. However, the National Crime Agency (no date) note that "[m]ore and more teenagers and young people are getting involved in cyber crime" noting reasons such as, the excitement and fun attached to crimes including unauthorised computer access, production and distribution of malware, and Denial of Service attacks through to individuals being unaware and unacquainted with the consequences and penalties of such crimes.

While this study shows some individuals were successful, for example, in receiving their money back others were not. One respondent reported crimes to who they felt was the relevant authorities/websites and noted "[n]o one was interested. Nothing. Lost money." This respondent recognised crimes to have occurred such as; "Phishing, false website similar to DVLA, accidental [illicit] adult-pop-up." While four other respondents expressed problems including irretrievable emails and no interest from their email host provider and crimes having occurred in another country through to "stolen devices [being] recovered [but] phishing emails still [happening] weekly [and] religious & ethnic hate groups websites still active because they got protected by free speech".

Analysis of the responses highlighted the need of wider awareness and educations of digital crimes and security. Participants noted having learned from the crime or from their own mistakes. Several respondents continued by expressing their views that society should be trying to tackle digital crime and cyber security through "education", expressing how they believe there are "[s]o many people [who] don't understand digital crime" and that in their own circumstances how they "secured all [their] accounts regardless of the type of breach that occurred and learned from [their] mistakes."

While the need for more awareness of crime and prevention is shown, there is also the need for education and awareness to combat the anxiety and worry these incidents may invoke on the public and victims of such crime. One respondent who became a victim of crimes such as, phishing, online fraud and malicious software said they were "dubious of [computer/Internet] use" as a result. This study cannot confirm that every victim felt some level of anxiety after their troubles, however, further study should consider if previous victimisation leads to different behaviour online.

3.2 Participant views on what should be tackled in society considering digital crimes and cyber security

Several responses to the question over societal changes focus on the need for the public to understand the nature of digital forensics and cyber security, along with the awareness and the image seen of a digital forensic practitioner. One respondent stated we should be looking to tackle "[t]he image of a forensics analyst … [they] are not NCIS … keyboard hackers." Another respondent stated "raising the profile of cyber/digital crime to show it is not victimless" is crucial, as well as "raising the awareness of how to protect [oneself] from digital and cyber crime. Providing free confidential and reliable advice to victims of cyber crime." A respondent aged 25-30, who has not been affected by digital crimes, summarises the need for "an established mid-ground where the Internet can be used properly", expressing how, "the digital age has made it far more easy for people to negatively impact people's lives while at the same time being a valuable asset."

Responses from the public were open coded into categories which most suited the items stressed e.g., education, specific crimes, and punishments. These were then categorised into groups of similar topics. Analysis of responses shows, knowledge (including awareness and education) accounted for 71 occurrences, followed by crime and punishment with 26 occurrences. 19 responses related to security and prevention while 11 responses related to control (e.g., policing, monitoring and responsibility). Finally, seven were attributed to society (particularly the need for respect).

General public awareness of digital and online crime and attitudes towards security online were a concern which participants called into question; where awareness was categorised on 43 occasions. A few respondents felt some people in society place less emphasis on the security of their personal data online and on devices compared to more physical counterparts such as traditional use of paper and keys for information and storage. One person commented: "awareness among general society of the vulnerabilities needs to be improved, and the possible consequences to individuals affected made clearer". Awareness noted by participants included the need for individuals to become more accustom with preventative measures, potential criminal acts, the associated affects and responses required to such crimes. While another respondent highlighted the idea of "making people in general aware as to how easy it is to gain [their] information [and] how liberally people use the Internet without realising they could be passing on their information unwillingly." One respondent stated "teaching 3 stages of defence: prevention, incident management, consequence management" are central to tackling societies approach to security and online information.

In addition to awareness, education was categorised on 25 separate occasions with two respondents pinpointing the necessity for education to target the youthful. They believe schools should teach and "involve younger generations in digital crime prevention" to protect the adolescents from sharing too much information, and from crimes such as, cyber bulling, abuse and harassment. One respondent argued how "more responsibility [should be] placed in the hands of those making millions out of the Internet". For example, much larger and well-known corporations including Google and Facebook to help "provide sufficient protection".

This is an interesting debate on where the responsibility lies, and to what degree responsibility should be weighted toward individuals, Internet-based companies, the criminals, the victims and governing authorities. This paper does not look to answer this question in-depth due to its vast breadth and uncertainty. However, there have been several news stories, most notably the Facebook and Cambridge Analytica scandal (Information Commissioner's Office, 2018) which have heightened the need for companies to take responsibility for their actions. Consumer trust is centred around ensuring personal data is secure and an argument for transparency in data use, particularly when it is almost inevitable that data breaches will occur is suggested. Along with the need for more transparency on who and what data can be accessed, collected and used in terms of information is the need for what three respondents note as respect towards others and their belongings.

The idea of transparency suggested in this study is targeted at businesses and what criminals can access if a breach were to occur. Often, concerns are targeted towards what businesses or institutions hold in terms of Personally Identifiable Information (PII), particularly stressed with the recent introduction of the General Data Protection Regulation (GDPR) and the potential for malicious access to such data. Although one respondent also notes the need for "transparency" in terms of the data law enforcement can access. The respondent states "more transparency in who has access to what information – so we know what the government/police etc., take from us [and] know from us." Broadly speaking there is a trade-off between the amount of data governing bodies and law enforcement can obtain with the number of individuals, length of time it takes as well as how intrusive an investigation may be. As a result, it is highly unlikely that such bodies are spying on people 24/7 if not only for the resource limitations.

Another respondent expresses the need for "less sweeping powers by the state" and the requirements for "updating appropriate legislation" to combat issues such as "Cyber bulling, copyright issues, self-censorship and the 'social cooling' effect" where they believe there needs to be a "mass education of 'cyber sec' from a young age". In contrast to the views for less sweeping powers that downplay the role of investigatory powers, one respondent portrays the view that everything should be tackled. They express that they "think digital crime is only going to get worse and at the moment the police are perhaps a little ill-equipped to deal with this". This point makes for interesting discussion and shows a level of mindfulness of the position, particularly in public sector roles, towards resourcing, staffing, funding, skills and time within digital forensics and security roles.

Although anxieties were shown by a minority of respondents towards too much 'snooping power' (e.g., what data governing bodies can access) other respondents provided views such as the need for stricter monitoring and access controls, more monitoring and policing and the development of stronger penalties and punishments, reduction in anonymity online (for more advanced users), greater visible policing online, an aggressive pursuance of hackers, better public awareness, training and education and restriction on use of the Internet for those who commit crimes in addition to time served.

Note it is not just awareness by the end users that participants call into question, with responses such as tackling "the actual source of criminal activity". Concerns that "security risks are not taken as seriously as they should be" and that people need to become accustomed to preventative techniques they can use to help secure their devices and systems resonated with many participants. Some noted how there specifically needs to be more support and availability of information for much older generations to understand the Internet, devices and security. More commonly, security-based responses linked to knowledge (i.e., people being more aware of security measures and being educated to protect themselves). Security for some respondents linked to stronger punishments for criminals accessing and distributing information where one respondent discusses security is not just about people's device security but data security, articulating "websites are more secure and harder to hack, it's becoming more common for information to be leaked and personal identities stolen". Although there is no statistical evidence to prove or refute the participant's claim and the rise in data breaches, ransomware and cryptocurrency-themed attacks highlight the need for better security all-round.

It could be argued that several items listed above might not be necessary if, as a society, we could use education to tackle the motivation to commit a crime. That said, committing a crime has long existed both with and without the addition of technology. Regrettably, neither education, nor reformation, has been able to fully diminish peoples' motivations. The vast depth and breadth of the Internet has only enhanced the capabilities of criminal activities in other dimensions and resources. This raises the question: what people in society, professionals, governments and bodies can do to tackle this.

One individual remarked "there is so much freedom for all users on the Internet. I really do not know what can be done" with another stating, "I wouldn't know where to start in answering this". This is not surprising. However, there were only 8 occurrences where people were unsure or did not know what should, or could, be tackled within society in relation to online/digital crime. This is interesting as participants within the survey identify responses which show a conscientious nature toward the need for change and response to security issues.

3.3 Participant views on criminality and what law enforcement need to tackle in relation to digital crimes

Due to the ever-growing nature of digital devices within criminal activities and online crimes, it is recognised that digital and online traces are used in multiple facets throughout investigations within law enforcement. Participants were asked for their views on what should be focussed on. Responses were coded by criminal activity to identify topical and highly important crimes which this sample of participants feel should be addressed.

Categories were formulated using the tally of crimes noted. For instance, 'Theft' included examples such as identify theft/fraud, theft of data and any single instance of the term theft. Many of these categories were created taking into account crimes outlined in Section 3.3 of the UK Cyber Crime Strategy Home Office (2010, p. 11), a strategy which highlights financial (e.g. online fraud, identity theft, intellectual property theft and data security) and non-financial crimes (e.g. threats to children, hate crimes and political extremism). All of these are noted by participants in this study. Figure 2 represents the crimes categorised by occurrence (e.g. number of times mentioned) from high to low by this sample of respondents.

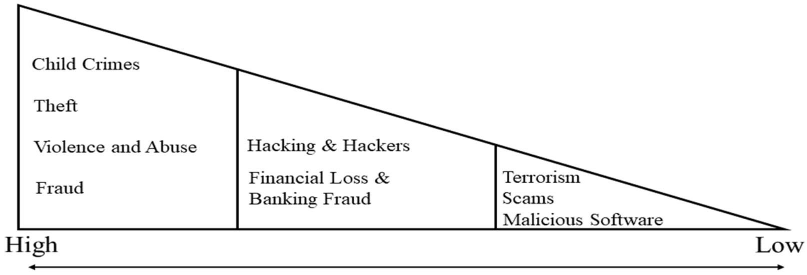

Figure 2: Occurrences of respondent identification toward online crime police officers should be tackling

The highest mentioned crimes were those relating to the harm of children (36 occurrences - e.g. grooming, abuse, illicit and indecent materials and exploitation), followed by theft (32 occurrences - e.g. identification and data theft), violence and abuse (24 occurrences - e.g. discrimination, hate crime, bullying and harassment), fraud (23 occurrences - e.g. fraud and insurance fraud), hacking (18 occurrences) and financial loss (16 occurrences - e.g. bank fraud and money laundering). What should not be inferred from Figure 2 is that the crimes least mentioned are less important to this sample of participants; this is not suggested by the respondents.

Data security, the awareness of preventative measures, and the awareness of online crimes were, again, mentioned by participants in societal change as well as by police officers. One expressed how they felt law enforcement should be tackling "any criminal activity via digital means [and] helping give crime prevention advice and assistance." Several responses were relatively vague; for example, "All of it"; "All"; "All Cybercrime"; "Anything that is meant to harm people" and "All! It is a crime". A total of 24 responded with this type of response. On the other hand, there were several individuals who noted all crimes should be tackled, while recognising that tackling all online/cyber-crime "is not a credible reality". While infeasible to tackle all crimes, a few respondents epitomise how in their own opinion, they view that some crimes are more important than others. Where some note how "as much [crime] as possible, from areas like child exploitation and fraud to simple "trolling" of people for no reason" should be focused upon. Of these responses, theft and fraud were highly prioritised.

4 Limitations and Future Work

One limitation of this study is its relatively small sample size. Further research should look to obtain more responses, looking to identify patterns in the crimes which individuals feel should be tackled in addition to the view that there is a need for greater awareness and education. Additionally, a minority of responses showed concerns and need for more accountability and clarity of access, storage and use of peoples' data in the hands of companies and governments and inferred during the investigation of a security breach. Future works to determine peoples' perceptions on accountability, responsibility and clarity of data after implementation of the General Data Protection Regulation (GDPR) should be considered in line with cyber security and digital forensics.

5 Conclusion

The number of individuals, both in this survey and captured using national statistics, who have fallen victim to digital crimes demonstrate continued concerns surrounding need for further education and awareness. Knowledge (including awareness, education and training) were the most highly themed group in tackling digital/online crime in society. Other responses focussed on measures of control and punishment. To enforce these actions continuous development and expansion of cyber security and digital forensic workforces is required. Some respondents note or infer that the demands and resources required to tackle digital and online crime are met with challenges in keeping abreast with continuous advances, and the unrealistic nature of being able to confront and investigate all criminal activity promptly. Analysis of individual responses support the ever-greater need for practitioners within the disciplines seeking to combat digital crime. Respondents within this study felt that crimes associated with children, fraud and theft and, violence should be at the top of the list for law enforcement when investigating digital/cyber related events. The peoples' perceptions, based on this sample, also focussed on transparency and awareness. This included a range of target audiences where tackling awareness of the impact of criminal activities, through to the use, collection and storage of data by companies and governments were key themes across responses.

6 References

Cambridge University Press (2013) 'keyboard warrior, n.', *Cambridge Advanced Learner's Dictionary and Thesaurus*. 4th edn. Cambridge: Cambridge University Press. Available at: https://dictionary.cambridge.org/dictionary/english/keyboard-warrior (Accessed: 22 February 2019).

Home Office (2010) *Cyber Crime strategy*. Norwich: The Stationery Office (CM 7842). Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228826/7842.pdf (Accessed: 4 March 2018).

Information Commissioner's Office (2018) 'Findings, recommendations and actions from ICO investigation into data analytics in political campaigns', *Information Commissioner's Office (ICO)*, 11 July. Available at: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/07/findings-recommendations-and-actions-from-ico-investigation-into-data-analytics-in-political-campaigns/ (Accessed: 15 August 2018).

Murphy, J. and Roser, M. (2019) 'Internet', *Our World in Data*. Available at: https://ourworldindata.org/internet (Accessed: 15 April 2019).

National Crime Agency (no date) *Cyber crime: Preventing young people from getting involved in cyber crime*, *National Crime Agency*. Available at: http://www.nationalcrimeagency.gov.uk/crime-threats/cyber-crime/cyber-crime-preventing-young-people-from-getting-involved (Accessed: 22 February 2019).

National Crime Agency (2016) *Cyber Crime Assessment 2016: Need for a stronger law enforcement and business partnership to fight cyber crime*. 1.2. London, United Kingdom: Strategic Cyber Industry Group (SCIG). Available at: http://www.nationalcrimeagency.gov.uk/publications/709-cyber-crime-assessment-2016/file (Accessed: 17 February 2018).

The Office for National Statistics (2018a) *Crime in England and Wales: Additional tables on Fraud and Cyber crime*. Available at: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesexperimentaltables (Accessed: 17 February 2018).

The Office for National Statistics (2018b) *Crime in England and Wales: year ending September 2017*. Available at: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingseptember2017 (Accessed: 17 February 2018).

The Office for National Statistics (2019) *Crime in England and Wales: year ending September 2018*, *Office for National Statistics*. Available at: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingseptember2018#computer-misuse-offences-show-a-decrease-in-computer-viruses (Accessed: 11 April 2019).