

We are IntechOpen, the world's leading publisher of Open Access books Built by scientists, for scientists

6,300

Open access books available

170,000

International authors and editors

185M

Downloads

Our authors are among the

154

Countries delivered to

TOP 1%

most cited scientists

12.2%

Contributors from top 500 universities



WEB OF SCIENCE™

Selection of our books indexed in the Book Citation Index
in Web of Science™ Core Collection (BKCI)

Interested in publishing with us?
Contact book.department@intechopen.com

Numbers displayed above are based on latest data collected.
For more information visit www.intechopen.com



Chapter

Classification Models for Preventing Juvenile Crimes Committed with Malware Apps

Joshua Ojo Nehinbe

Abstract

Spectacular developments that were recorded in the field of software engineering in recent years have led to the influx of software industry with series of computer apps such as dating apps, games apps, entertainment apps, banking apps, Photoshop apps, meetings and virtual conferencing apps. Studies have shown that most computer apps are widely accessible to adults and juveniles to download and effortlessly navigate through them. However, researchers have now revealed the existence of malware apps as new groups of computer apps that are strongly competing with legitimate computer apps and the latest rates at which some juveniles can adopt them to commit crimes. These discoveries have raised serious doubts about the elements of the crimes, the circumstances that surround vulnerable children to commit the crimes and how these dilemmas are rarely buttressed by pragmatic studies over the years. This chapter adopts mixed methods to critically explore the above issues. Qualitative interviews of 60 teenagers (between the ages of 10 and 17) and 20 grown-up children (between the ages of 18 and 22) together with 5 professionals were carried out. The analysis extended the generic elements of juvenile crime and raised new legal dilemmas regarding the concepts of transfer of criminal liability, compelled (or obligated) liability, 'act' that constitutes juvenile crimes and the restrictive applicability regarding criminal consent of extremely young children that are still under the tutelage and guidance of their parents.

Keywords: crime, juvenile crime, Malware apps, intruders, computer crime, suspects

1. Introduction

The spectacular developments recorded in the field of software engineering over the years have directly led to the influx of the software industry with series of computer apps such as dating apps, loan apps, games apps, entertainment (or music) apps, image editing apps, cloud data storage apps, messaging (or messenger) apps, discord apps, virtual workspace apps; password managing apps, scanning apps, antivirus apps, backup apps, video streaming apps, TV shows apps, codes and scripting apps, language learning apps, banking apps, cloud apps, presentation apps, reminders apps; apps for apps designers, Photoshop apps, meetings (or virtual) conferencing apps,

zip file apps and task-management apps [1, 2]. The beauty of these computer apps is that significant numbers of them are widely available and accessible to adults and juveniles to download and easily navigate through them. Nonetheless, market research has shown the existence of malware apps that are identified as new groups of computer apps that are strongly competing with legitimate computer apps in the software industry in recent time [3–5].

Serious dilemma has also been expressed in recent years on the fact that the scales of the operations and the levels of data security that companies and their respective service providers can jointly offer to customers (users of their services) across the globe are not the same. These tropical issues have pointed out the likelihood of future debates on the usage of criminal laws and or civic laws to adjudge corporate liability and the impact of overseas jurisdictions in criminal proceedings regarding juvenile committed crimes with offshore (or onshore) malware apps. Besides, juvenile crimes are long-standing social problems but the recent surveys have further compounded the problems [3, 4, 6]. Several empirical conclusions have now shown that the above advancements are facing serious threats and firm criticisms across the globe given the prevalent cases and sudden surge in the menace at which some juveniles can now adopt malware apps to commit crimes [7, 8].

Fundamentally, contemporary studies believe that juvenile is a social concept to describe adolescent or the characteristics of children and young people that have not fully attained the age of maturity [9, 10]. Children that are below the age of 18 are mostly categorized as juveniles in most societies [11]. A crime is defined as an act that is prescribed to be unlawful by statutes or criminal laws of a state or country [12–14]. Therefore, juvenile crimes connote unlawful acts that are committed by the children below the age of 18 years in the society [15, 16]. Malware apps are malicious software apps that are purposely created to have intrusive or criminally-minded motives. Malware apps, malicious software apps and malicious apps will be interchangeably used to connote the same concept in this chapter. Studies have further raised classical deliberations concerning the underlying motives of the designers of malware apps and their users. Studies on the capabilities of malware apps have shown that they can corrupt, explore, delete, deface, swindle and steal resources or personal details of another people. Some malware apps intend to distort the clarity of pictures and render them blurred. Empirical studies on software engineering have shown that malware apps can mute telephone conversations and suddenly turn them to be speechless or voiceless. It is a well-established fact that malicious software apps can make audio conversations inaudible to the participants in virtual conferences, virtual interview and virtual lectures. Another classical issue here is that the victims of various crimes that some juvenile can commit with malware apps may impact on just a person, two persons, more than two persons and more than one governmental body.

Several topical studies in the domains of criminal laws have also substantiated and categorically stated that juvenile crimes are social problems [10, 15]. Tropical issues in criminal laws have led to broad explanations of various elements of crimes and several considerations required charging or acquainting the suspects that are alleged of crimes over the years. However, apart from the fact that the concept of juvenile crimes committed with malware apps are emerging issues in the global society, there are clearly invalidated studies that have substantiated the correlations between the elements of these kind of crimes and the circumstances that surround the vulnerable children that may be alleged of the crimes, even in recent years [17]. The problems with these challenges are enormous. For instance, the actual causes and determinants of the above crimes are prone to oversight. The fear is that failure of some parents,

guardians and regulatory bodies to notice and counter the waves of the juvenile crime at an early stage may suddenly aggravate the effective supervision and 'the perceived level of misunderstanding of various forms' of the act [8]. Notwithstanding, social orientation, parenting, policing and social policy can begin to face strict criticisms in most civic settings if more and more youths are alleged of the juvenile crimes committed with malware apps [7, 8]. Agitations that will be calling for serious awareness through media and political participations may begin to surge in order to wakeup parents, guardians and police in their duties so that they can perfectly monitor vulnerable juveniles that may adopt malware apps to perpetrate crime or be victims of the crimes. The severity of the above problems is worrisome due to the inabilities of most governments and agencies to design suitable preventive interventions that will decisively curtail the emerging developments in the software industry. For these reasons, parenting and parental care as well as the efficacies of several social policies across the globe is generating increasing criticisms [8].

Another critical consideration is that most of the users of modern apps (especially employees) have little or no choice to determine the level of their participation and the information that they must supply to enable them use some of the modern apps that currently exist in the software industry. The reason is that most employers rarely involve their employees in the selection and evaluation of modern apps for supporting process flow at workplace. Instead, some employers often obliged their employees to use and wholeheartedly adopt them especially for scheduling, management of task, workplace meetings, virtual events (e.g. conferences, workshops and lectures), official reporting and chatting with colleagues or bosses, etc. with the view of boosting productivity, sales and profitability. Given the fact that Internet and all computer apps have inherent vulnerabilities, bugs and vulnerabilities that may not be conspicuously known to software experts to fix, on these reasons, the security of the entire components of the above apps and the level of the protection they can offer to the end-users that have trusted (or were compelled to trust) and sincerely adopted them begin to attract the attentions of criminologists, legal and security experts [8, 18].

Industrial dispute and conflict resolution among software companies, victims and service providers and how to amicably resolve them are now raising serious legal and technical debates especially, if it appears that computer apps that users sincerely trusted have aided or assisted criminals to achieve their malicious motives. The above legal and software issues are raising legal dilemma about the issues of compelled (or obligated) liability due to an assurance from a third party applications and the actual organization that an employee that incurs harm from computer apps can actually sue between their employer and the vendors of computer apps that seems to have aided the crime. Some school of thought may believe that service providers can be penalized by law for not doing their jobs well. The fact is that employees may be punished for refusing to embrace the modern apps obliged by his/her employer. So, another school of thought may argue the above scenario on the basis of the 'commission' or 'omission' as a possible element of the crime. In this circumstance, the question of whether the law is justified to penalize or absolve the employer and or their service providers, and then dismiss or award compensation(s) to the employee requires deep legal technicality of these new kinds of cybercrimes [12–14].

Despite of the existing standards of software methodologies, it is impossible to rigorously protect different computer apps in the same way and especially given the fact that computer apps are designed and manufactured by different vendors [19]. For instance, copyright, Intellectual Property (IP) and trade laws usually prohibit

two different software companies from copying their designs, underlying theories, principle and cryptographic algorithms that they adopt to protect the passwords and messages in transit. Thus, some computer apps will surely have inbuilt security features than another [19]. So, the level of computer crimes that intruders can commit with them equally varies. The fear is that collaborative empirical reviews had earlier warned that the above problems can increasingly metamorphosed into complex problems that will compound the detective and preventive interventions for various kinds of juvenile crimes committed with malware apps in the next decade if the global society erroneously allows them to escalate to high levels [8, 17]. Consequently, the initial motives of the designers of computer apps have begin to suffer wider criticisms in a recent time.

Another puzzling dilemma that can be confronting most software and legal experts is to establish the correlations between the elements of the above juvenile crimes with malware apps and the circumstances that surround the vulnerable children that are rarely buttressed and made explicit by empirical studies on juvenile crimes over the year [17]. For this reason, the objectives of this chapter are split into three groups. The chapter intends to explore the causes of juvenile crime committed with malware apps. The chapter also intends to state various 'act' that can constitute infringement and classified as juvenile crimes committed with malware apps. The chapter intends to adopt the above objectives to propose empirically proven classification models to simplify and explicate the above legal and social dilemmas.

By using mixed methods and quantitative interviews, 60 teenagers (between the ages of 10 and 17) and 20 grown-up children (between the ages of 18 and 22) together with 5 professionals were recruited to explore the above social problems. Quantitative analysis of logs of Snort Intrusion Detection Systems (SIDS) was incorporated into the mainstream of the sessions of the interactions with the above participants. Thereafter, we thematically analyzed the results obtained. One of the contributions of this chapter is that it has extended the generic elements of juvenile crimes and further suggested various determinants of the circumstances that may surround vulnerable children to commit juvenile crimes with malware apps. The chapter has further empirically substantiated the correlations between the determinants of the circumstance that may surround vulnerable children and the elements of juvenile crimes with malware apps. The paper also introduced new legal discourses and then offered suggestions to lessen parenting hurdles and how to countering the weaknesses that may be inherent in the policing and social policies on the above category of global crimes. The remainders of this chapter are organized as follows. Section 2 discusses the domain of coverage of modern computer apps. The section also opens up new legal dilemmas on computer apps. Section 3 explains the rudiments of juvenile crimes committed with malware apps. The section further itemizes the generic elements of most crime scenes. Section 4 discusses the methodology of the survey. Section 5 states and analyses the results and their implications. Section 6 concludes the chapter. The chapter also offers suitable areas that researchers can explore to extend the research that is reported in this chapter.

2. Modern computer apps

Computer application programs are often abbreviated as computer apps [1]. Legitimate computer apps in the software industry can serve a wide collection of functions and purposes to the target audience [1, 2]. Some legitimate apps enable

their users to view, upload and share favorite songs and new albums of artists with friends and social groups. There are modern apps that enable people to have access to audio-books, historic podcasts, video, motion pictures, selected artifacts and read, examine or watch them at their leisure time. Some modern computer apps enable users to create their personal accounts, sign on to the apps by using their personalized accounts and remotely connect to some companies, colleagues and professionals in other locations and engage in virtual conferencing.

The functionalities of some of the accessible modern apps in the software industry allow their users to also add or invite people (users) as contacts [1]. Some computer apps allow users to select the kinds of services (such as message or call) of their choice. Some apps can enable users to equally share files and log on to chat box and engage in private or official conversations. Some of the existing apps enable their users to customize and fine-tune their background information. Some computer apps permit users to upload their personal pictures and insert personal notes or personal ideologies on their chat profiles. Some modern apps can engage participants and host many interactive sessions. Besides, some computer apps can engage several participants in every session and they will still experience clear pictures and audible audio conversations.

More so, the current advancements in computer apps cut-across scores of human domains. For example, there are computer apps for modern photography subsumes taking pictures (photographs or photos, snapshots), cinematography (movies production), film production, picture production, animatronics (animation), computer graphics, shooting cartoons, moving picture, mood mining, printing and camera repair. Furthermore, legitimate apps such as printing apps can enable both the professional and amateur printers to increase their creativities and proficiencies in photography. Nevertheless, the striking issues on modern computer apps are worrisome. The issue of privacy control and virtual data sharing syndrome have made some experts to reserve their comments on the confidentiality, integrity, availability and non-repudiation of virtual signals that would have migrated through several networks in different intercontinental boundaries in the course of using most of the existing legal computer apps. Another concern is that unproven juveniles that are suspects of the intrusions into computer apps may (or may not) necessarily commit the offense. Some juveniles may not possess software engineering skills that they require to design apps that will conform to best global standards. For these reasons, the foreseeable impacts and the confidence that users usually have in computer apps are constantly threatening the trust, customers' loyalty, recommendation and continuous usage of the current groups of computer apps in the software industry.

The legal interpretation and the technicality of cases of violations and misdemeanors regarding modern computer apps have now raised four pondering issues that require lateral deliberation and special attentions [3]. Firstly, the emergence of accidental (inadvertent, unintentional or unplanned) damages that can be incurred by end-users based on "the services and the trust in computer apps", especially if the events are proven (or suspected) to be directly caused by the occurrence of unexpected intrusions against the modern computer apps they use must require in-depth legal consideration. Secondly, the criminal consent of underaged children demands urgent review in law books and contemporary bulletins. Thirdly, the issue of transfer of criminal liability in the circumstances of using an apps and getting into "avoidable trouble" and fourthly, the circumstances whereby some legitimate apps may be held (or charged) by complainants for being liable to have criminally permitted some juvenile crimes (that left the victims with severe impacts) to have permeated (infused, pervaded) or

spread through them. After all, some statutory laws legalize complainants to institute legal actions against some manufacturers of items (or products) for the accidental (involuntary or unexpected) damages they have incurred by virtue of the trust they have in their products (or services) and in the course of using their products, services or items. The above legal paradigms and discourses are new debatable issues that we have put forward in this chapter to the criminologists and legal experts in the domains of computer apps to critically explore [8].

3. The fundamentals of juvenile crimes committed with malware apps

The crime itself and its elements are two inclusive components of juvenile crimes with malware apps. Unlawful acts that can constitute juvenile crimes are subsets of cybercrimes [7]. Studies on minor offenders converge and affirm that juvenile offenders are mostly tried in juvenile courts [15]. Cybercrimes are various crimes that perpetrators commit by means of digital devices (such as computers and mobile phones) and Internet facility. However, most studies on juvenile crimes that relate to cybercrimes are inexplicit and they are often reserved on the various manners that vulnerable children can be accused of breaking (or to have attempted to break) cyber laws with malware apps [11]. Rather, most contemporary studies simply treat and group the majority of the children that are alleged of cybercrimes as minor offenders (or minors that are suspects of cybercrimes).

Investigations of crime and the outcomes of the proceedings of criminal courts can be used to classify juveniles that are held as suspects of crimes committed with malware apps [10]. Basically, an offender is a term that represents a lawbreaker, delinquent or criminal. Thus, juveniles are treated as minor offenders in criminal courts [17]. A child that has been proved by courts of competent jurisdiction to have contravened cyber law(s) for the first time is known as first-time offender in cybercrime. In the same way, a child that has been proved by courts of competent jurisdiction to have consistently contravened any section of cyber laws is often called habitual offender in cybercrimes. In terms of recovery strategy, the above two groups of juvenile offenders obviously require different therapeutic interventions. In effect, rehabilitative and punitive interventions for the above settings must be commensurate to the offenses committed by offenders in order to strictly comply with Human Right laws.

3.1 What is juvenile crime committed with malware apps?

There are lots of juvenile crimes and many reasons that may lure or encourage young children to commit crimes with malware apps [10]. The bottom line of these issues is that any act of infringement by juvenile with malware apps is a crime in this respect. Infringement can be defined as an act of violation or misdemeanor and such act usually disregards ethical agreement or moral uprightness. For examples, a child that uses malware apps to unlawfully break into the telephone or computer system of another person, or steal, corrupt, modify or update the information in the electronic device(s) of another person can be alleged of crimes committed with malware apps. Additionally, a child can be alleged of juvenile crimes with malware if he/she decides to send unsolicited and offensive mail(s), insulting text(s), disgusting image(s), nasty call(s), threatening call(s), intimidating mails, etc. with malicious apps to a person that regards the 'act' as offensive and feels insulted with the 'act'. In addition,

a child that uses unapproved apps to share and disseminate the picture(s) or blog(s) of another person, (either knowingly or unknowingly) in an offensive manner, or uses malware apps to steal the identity of another person with malware, or he/she uses malicious apps to sell contraband items or stalking innocent person(s) with malware can be alleged of juvenile crimes with malware apps.

Moreover, a child that uses malware apps to disrupt the business operations of a private person or corporate organization(s), or uses malware apps that behave in the manner that resembles malevolent computer programs (either local or indigenous computer program(s), foreign or proprietary program(s)), can equally be alleged of committing juvenile crimes with malware apps. Not only that, a child that uses malicious apps to harm (or intend to harm) another person(s), or uses any malware apps to spread computer viruses, Trojans, worms, etc. across computer or mobile networks may be alleged of juvenile crimes with malware apps. Fundamentally, a child that uses malware apps to unlawfully install (or he/she is caught while requesting for information to install) spyware in a computer or mobile phone of another person or organization's networks can be alleged of committing juvenile crime with malware apps. There are strong contestations pertaining to the legality of the fact that juveniles are socially categorized as adolescents, minors or teenagers in civilized societies. For this reason, contemporary studies argue that the ages of juveniles can technically qualify them to be accorded with the same treatment and honor that characterized the young people that their ages belong to the beginning of puberty and maturity age in the society. With these stacks of controversies, the statutory consent of the alleged minors or teenagers to be 'old enough' to discern (or must have known) malware apps and all actions that premeditate juvenile crimes in the process of using computer apps require rigorous legal interpretations.

3.2 Elements of juvenile crimes with malware apps

Studies have made known that juvenile crimes committed with malware apps can involve many elements [10, 20]. The term elements of juvenile crime describe various circumstances that surround or underlie the crime that are defined and recognized by the statutes or laws of a given state (or nation) or international court of justice. In other words, the statutes of each sovereign state usually set what should be the elements and the limit of juvenile crimes. However, studies have shown that juvenile crimes with malware apps are novel areas that have not been completely proved in pragmatic manners over the years.

Figure 1 illustrates the generic (standard) elements of juvenile crimes with malware apps [17, 21]. According to Britannica [22], consideration of the generic elements of juvenile crime should revolve round the conduct of the child (or criminal act), the mental state of the mind of the accused child at the time of the conduct (criminal intent), concurrence (agreement/disagreement to perform the 'act') and the causation between the conduct of the child (act) and the effect of the 'act' (criminal liability) either there is victim (s) or there is no victim involved (in case of victimless crime) [23].

Nonetheless, some of the social and legal components of the above elements of juvenile crimes remain debatable over the years [17]. The premise of this chapter is that investigators, prosecutors and judges must not expend huge resources to clearly unravel juvenile crimes committed with malware especially if the crimes are not properly split into their elements. The above standard elements are also common to

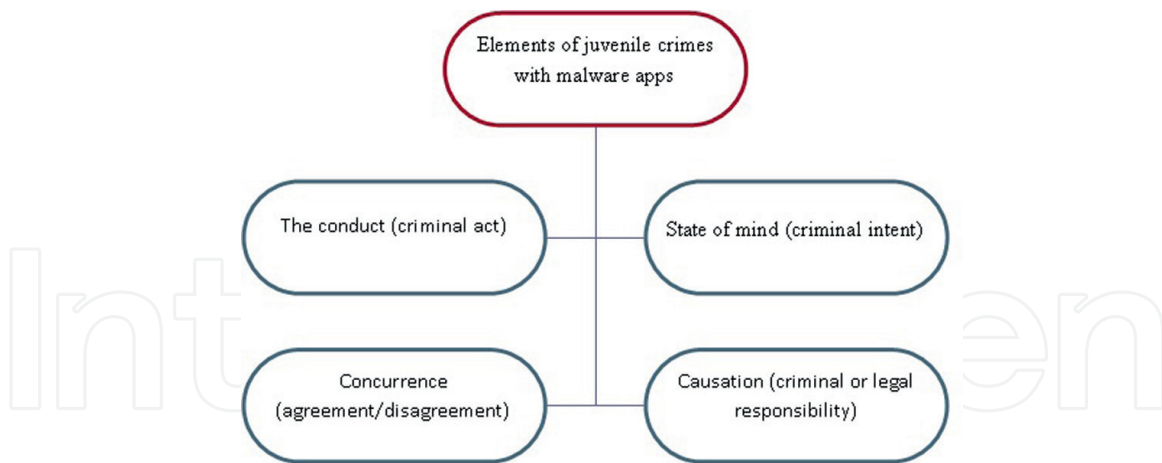


Figure 1.
Generic elements of juvenile crimes with malware apps.

most crimes. They are usually defined in criminal statutory books but prosecutors must be able to prove them beyond reasonable doubt in order to prosecute suspects of juvenile crimes. The above elements of juvenile crimes committed with malware apps may connote omission (neglect) by a child (voluntary act), commission (command0 (state of mind) of a child at the point of committing the act. A child can commit an act with malware apps voluntarily (intentionally) or involuntarily (unintentionally). For example, a child that intentionally uses malware apps to commit any of the above categories of crimes or related crime(s) is an example of voluntary intentional crime. Conversely, a child that unintentionally uses malware apps to commit any of the above categories of crimes or related crimes is an indication of involuntary or unintentional crime.

The minimum age that a child can be criminally held responsible for a crime usually varies but the internationally recognized range is between 6 and 18 years [16]. Furthermore, in a society where comprehensive justice systems exist for minor offenders (or may not exist), the prosecutor must be able to establish the legality of the fact that the child is criminally liable to be held responsible for the act especially if the allegation involves severe damage that is attributed to a child that is still below the above age range. That is, a prosecutor must be able to proof that it was through the direct participation of the child with malware apps that have done the harm or expected to have done harm to the victims(s). Detectives must be able to equally talk emphatically (while necessary) about the alleged malware apps must have been the root cause(s) of the allegation(s), or the investigative reports have traced or attributed the alleged malware apps to the accused child without any reasonable doubt.

Investigators may hold some children criminally liable (responsible) for certain juvenile crimes committed with malware apps for different reasons. Investigators may hold two or more children criminally liable for certain juvenile crimes in the above context if there are sufficient evidence, feelings and likelihood of accomplice in the allegation. Shared or joint criminal liability is a current legal issue in juvenile crimes with malware apps. This concept becomes relevant whenever a child deliberately (inadvertently) fails to act or prevent the act when in actual fact it is the legal duty of the child to act and given the fact that the child is capable of mitigating the crime at that particular instance. Ignorance is not acceptable in criminal laws. The question is whether the child is legally educated enough to ascertain and remove

the uncertainties that surround the level of his/her “inadvertently act” through the unawareness or awareness of his/her legal duties in the society. The second issues is whether the child can be charged (or not charged) for his/her failure to take action (or not to take action) in the context of criminal liability” are purely determined by the prosecutor, judge and the defendant(s) of the case.

Some criminal laws may not actually forbid children from playing with the mobile phones and Internet-enabled computers of their parents, guardians and fosters at home. So, the determination of the mental element (guilty mind) of the perpetrator (or a child accused of juvenile crimes committed with malware apps) and the issue of “joint criminal liability” among two or more children require rigorous exercises. This is because studies have shown that most statutory documents have not clearly clarified the concept of “guilty mind” in the above context.

A child that was playing with his/her parent’s phone may not have ‘purposely’, ‘recklessly’, ‘knowingly’, ‘negligently’, ‘carelessly’ or ‘neglectfully’ infringed the privacy of another person. The rationale for accusing, adjudging or acquitting a child of being guilty (or not guilty) of malware crimes may seem absurd in legal and media settings if the elements of the crime are improperly substantiated beyond reasonable doubt. The approach that media adopts to present and deal with the issue of juvenile crimes with malware apps and transmit them to the society worth consideration. This understanding is that the media has the power to reshape the youth and the society’s knowledge and understanding about juvenile crimes and social issues that come with them. These can in turn influence the formulation of regulatory legislations and their interpretations on the above social and legal issues. In essence, juvenile crimes committed with malware apps are subsets of other kinds of global crimes committed by vulnerable young and adult people. Yet, with inadequate legal frameworks in the global community, recent topical studies have shown that there are several refutable uncertainties about the above concepts and the statistical relationships of the entities that essentially constitute and underlie the various elements of the juvenile crimes committed with malware apps across the globe [16].

4. Methodology

The researcher recruited 60 teenagers (between the ages of 10 and 17) and 25 grown-up children (between the ages of 18 and 22) for the survey. The datasets for the survey were collected with the help of mixed methods and quantitative virtual interviews using emails and Whatsapp conferencing tool. The participants were presented with two different forms of the logs of Snort Intrusion Detection System (SIDS) in four virtual conferencing sessions to evaluate their level of understanding on network forensic investigations of computer and related crimes.

The first category of the logs of SIDS was raw forensic evidence of two different trace files that were collected from the spanning mode of the computer networks of a University for a period of 120 hours. **Figure 2** illustrates the second categories of the datasets and how forensic investigators can design log analyzers with C++ programming language to investigate forensic evidence.

The quantitative analysis of the above logs were presented to the children in four brainstorming sessions and the conversations focused mainly on crime investigations and how it is also possible for detectives to easily track and arrest the suspects of crimes committed with malware apps, cybercrimes or computer and related crimes. The statistical probabilities of the themes of the responses obtained from the

```

TCP Options (3) => NOP NOP IS: 45992 76816
Forensic evidence successfully processed.
Processing date is: 07/30/22
Processing time is: 21:01:16
708
TCP Options (3) => NOP NOP IS: 45992 76816
TCP Options (3) => NOP NOP IS: 45992 76816
08/03-02:47:13.870029 192.168.2.1:65086 -> 192.168.2.2:21
Forensic evidence successfully processed.
Processing date is: 07/30/22
Processing time is: 21:01:16
709
08/03-02:47:13.870029 192.168.2.1:65086 -> 192.168.2.2:21
Forensic evidence successfully processed.
Processing date is: 07/30/22
Processing time is: 21:01:16
710
08/03-02:50:18.800388 192.168.2.1:65167 -> 192.168.2.2:21
Forensic evidence successfully processed.
Processing date is: 07/30/22
Processing time is: 21:01:16
711
08/03-02:50:18.800388 192.168.2.1:65167 -> 192.168.2.2:21
Forensic evidence successfully processed.
Processing date is: 07/30/22
Processing time is: 21:01:16
712
08/03-02:50:18.820885 192.168.2.2:21 -> 192.168.2.1:65167
713
08/03-02:50:18.820885 192.168.2.2:21 -> 192.168.2.1:65167
TCP Options (3) => NOP NOP IS: 6596 46348
Forensic evidence successfully processed.
Forensic evidence successfully processed.
Processing date is: 07/30/22
Processing time is: 21:08:02
9800
76
08/04-20:31:08.384816 192.168.2.205:4081 -> 192.168.4.2:139
Forensic evidence successfully processed.
Processing date is: 07/30/22
Processing time is: 21:08:02
9801
44
Forensic evidence successfully processed.
Processing date is: 07/30/22
Processing time is: 21:08:02
9802
52
08/04-20:29:09.630009 192.168.2.45:32813 -> 192.168.8.2:21
Forensic evidence successfully processed.
Processing date is: 07/30/22
Processing time is: 21:08:02
9803
44
Forensic evidence successfully processed.
Processing date is: 07/30/22
Processing time is: 21:08:02
9804
76
08/04-20:22:44.839558 192.168.2.205:1217 -> 192.168.8.2:139
Forensic evidence successfully processed.
Processing date is: 07/30/22
Processing time is: 21:08:02
9805
44
Forensic evidence successfully processed.
Processing date is: 07/30/22
Processing time is: 21:08:02
9806

```

Figure 2.
Evidence of log analysis of forensic evidence that can indicate cybercrimes.

participants were also analyzed. The probability of a theme is the likelihood that the event will occur in a collection of other themes.

$$\text{Probability (P)} = \frac{\text{Number assigned to theme (event)}}{\text{Total number of themes (events)}} \quad (1)$$

In addition, the probability of occurrences is interchangeably used as the prevalence index in some instance in this chapter. The most significant of the findings in the above investigations are presented below.

5. Results and analysis of malicious apps

Virtual demonstration of crime investigation that was carried specifically discussed a total of 9805 forensic messages that may be indicative of unlawful activities in cyber laws with the participants. Further simulations showed that there are intrusion detectors, such as Snort IDS that organizations can install within the gateway to their networks in order to instantly report and log malicious events as they are occurring or migrating in and out of the networks with the participants. The experiments simulated that SIDS is capable of tracking malware apps and to further expose potential perpetrators of illegal probing of cyber physical systems. The results also showed the existence of malicious apps that intended to spy specific ports of digital devices, unlawful propagation of packets with extremely long parameters; intrusions with invalid File Transfer Protocol (FTP) commands at Disk Operating System (DOS) command line, intrusions that intend to flout the loading of certain web pages and hypertext links and intrusions that spy the Hypertext Transfer Protocol (HTTP) addresses were tracked by intrusion detectors. Furthermore, it was demonstrated that detectives can trail and arrest all the suspects of malware apps through the sources of malicious activities. The sources (or addresses) of illegal FTP messages that have packets with extended payloads that exceed beyond

the maximum length of packets that have been set up to migrate within the computer networks of a university, characteristics of malicious attempts that resemble criminal attempts to overload digital networks with deformed packets and the evidence of the detection of FTP command parameters that were malformed but intruders decided to overload the networks with them were spotted by the participants in the presentations. In addition, the simulation also revealed how it is possible for SIDS to detect unlawful attempts to crack the passwords of users of computer apps (or other software) with motives to gain illegal access and steal the passwords of users in the host that is running services such as Trivial File Transfer Protocol (TFTP). In addition, it was shown that the above toolkit can equally monitor, log and report malicious activities that indicate bad sessions, computer attacks on the Server Message Block (SMB) and intrusions that aim at slowing down (or delaying) the inter-process communication between two processes that can be running as background processes in different networks.

Additionally, from the responses of the participants, we identified and classified prominent malware apps on the basis of their coaching skills. The prevalent of fake coaching apps were sought in **Figure 3**. The observations pointed out that there were no clear winners among fake career coaching apps, deceptive dating apps, fake financial coaching apps and fake voice coaching apps. We also observed that fake moral coaching apps were not frequently detected and understood by significant numbers of vulnerable children. The figure suggests that fake career coaching apps has the prevalent index of 0.235 among the list of categories of common malware apps that are competing with legitimate apps in the software industry. Fake career coaching apps pose to be the meeting point of opportunities for progressive person in life. These apps offer career counseling on prosperous occupations (or lucrative work) that a person can undertake for a significant period of time. We noted that some of the variants of these malware apps also focus on personal development and self-development in chosen occupations. Respondents believed that some of these apps assumed the roles and responsibilities of professionals with the intention to offer useful advice and information on available vocations, job vacancies and employment opportunities in certain localities.

Similarly, the above empirical survey suggests that fake moral coaching apps has the prevalent index of 0.176 among the categories of malware apps that are competing with modern apps in the software industry. Fake moral coaching apps profess to be experts in moral discussions and ethical dimensions in the civic society. These apps are designed to present principles of right and wrong behavior to the target audience. They pretend to frown at dishonest and immoral acts in the society. Some of the existing fake moral apps are holding or manifesting themselves as the authorities with high principles and

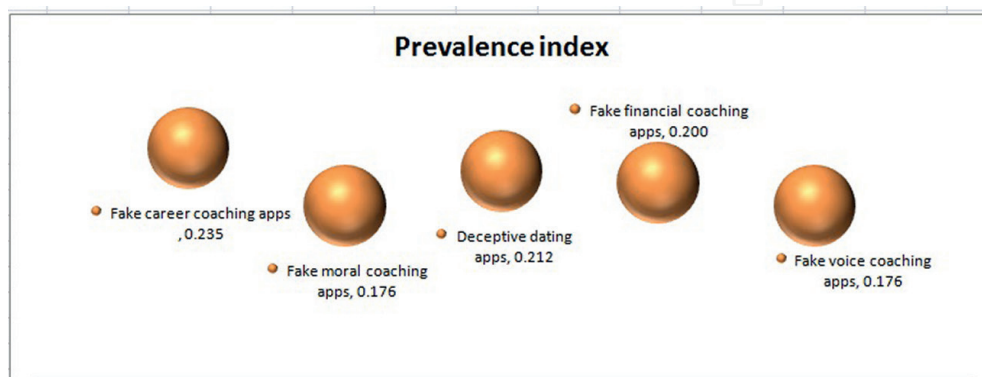


Figure 3.
Categories of malware apps competing with legitimate apps.

custodians of high moral standards that online users should consult whenever they need to seek for advice, directions and suggestions on proper conduct. The variants of these malware apps often pride themselves on being highly educated and knowledgeable in contemporary issues, moral and ethical values whereas, they are dishonorable apps and their underlying intention is to radicalize young children. Fake moral coaching apps achieve their malicious motives by gradually focusing on discussions about radicalization like ideological concepts, religious fanaticism and social criticism.

Figure 3 also put forward the idea that deceptive dating apps has the prevalent index of 0.212 among the categories of manware apps that are competing with genuine apps in the industry. Significant numbers of the respondents believed are several fake dating apps in software industry. The results showed that some fake dating apps can pretend to offer courtship, sex education and dating tips that will assist young children to find the right partners and improve their successes in dating and future relationships. These malicious apps can pretend (or operate) as if their ideas, theories and concepts will definitely assist young children to build happy, satisfying and successful future relationships. Some fake dating apps have inbuilt stages of romantic relationships for two individuals to engage in romantic activities together. Some fake dating apps come with criteria that vulnerable youths can adopt to evaluate their partner's suitability for future intimate relationship. The studies showed that the variations of the above apps can adopt romantic terms and slogan to thrill vulnerable kids.

These above observations recommend that fake voice coaching apps has the prevalent index of 0.176 among the categories of manware apps that are competing with justifiable apps in software industry. Fake voice apps are manware apps that pretend to be coaching children on mastery of sounds, accent and mode of speech in certain settings owing to adopt the data they gather from vulnerable children to defraud some people and swindle some vulnerable friends and the relatives of the users in later time. Some of these fake coaching apps can also request patronizers to introduce the apps to their friends and relatives. But then, the apps are secretly devising strategies to impersonate their users by using their voice, accent, pronunciation and patterns of intonation of the victims. Thereafter, the apps may masquerade and cause serious conflicts between the vulnerable children and their relatives. These apps pretend to be experts in vocal chords, pronunciation and sounds. Some of these manware apps indirectly introduce children to certain suspicious phone numbers that can require bio-data and bank details from the targets.

The observation also implies that fake financial coaching apps has the prevalent index of 0.200 among the categories of manware apps that are competing with genuine apps in the software industry. These groups of manware apps pretend to be experts that are willing to assist indigent children to overcome their financial difficulties and attain their aspirations in life. Sometimes, these apps can deceptively extort vulnerable children by stylishly requesting for token fees for the registration of participants in order to facilitate logistics.

Figures 4–7 establishes the correlation between the elements of the crime and the circumstances that may surround vulnerable children to be alleged of juvenile crimes with malware apps. **Figure 4** basically reveals that the act of vindictive, disconsolate, failures, misfortune, castaway, down grading and downcast can create unwholesome and objectionable circumstances for vulnerable children to be alleged of juvenile crimes with mobile apps. **Figure 5** suggests that news of failure, parental death, planned impulses and unplanned impulses can further constitute derived determinants of the circumstances that can influence vulnerable children to be alleged of juvenile crimes with mobile apps.

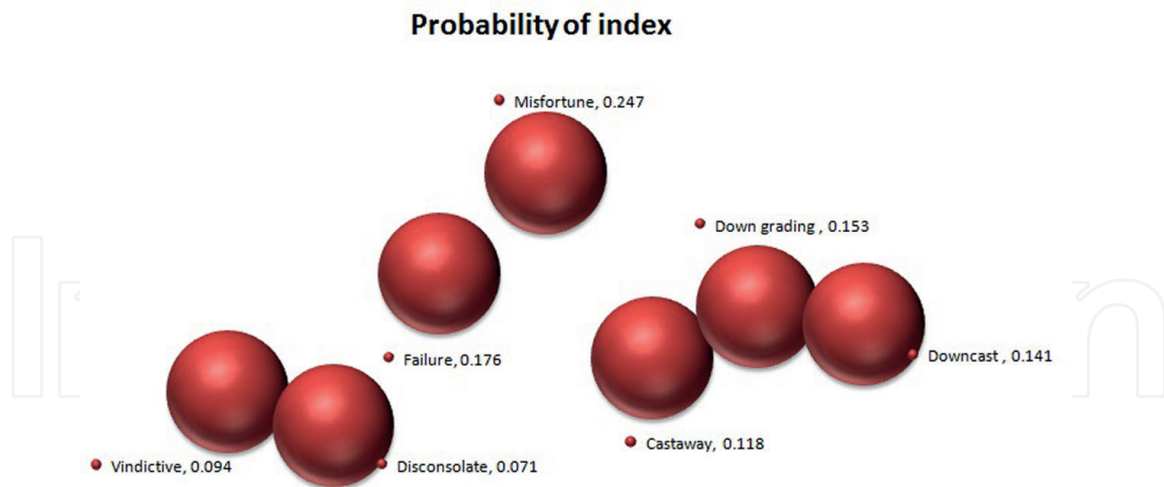


Figure 4.
 First category of rationale that underlie the elements of juvenile crime with malware apps.

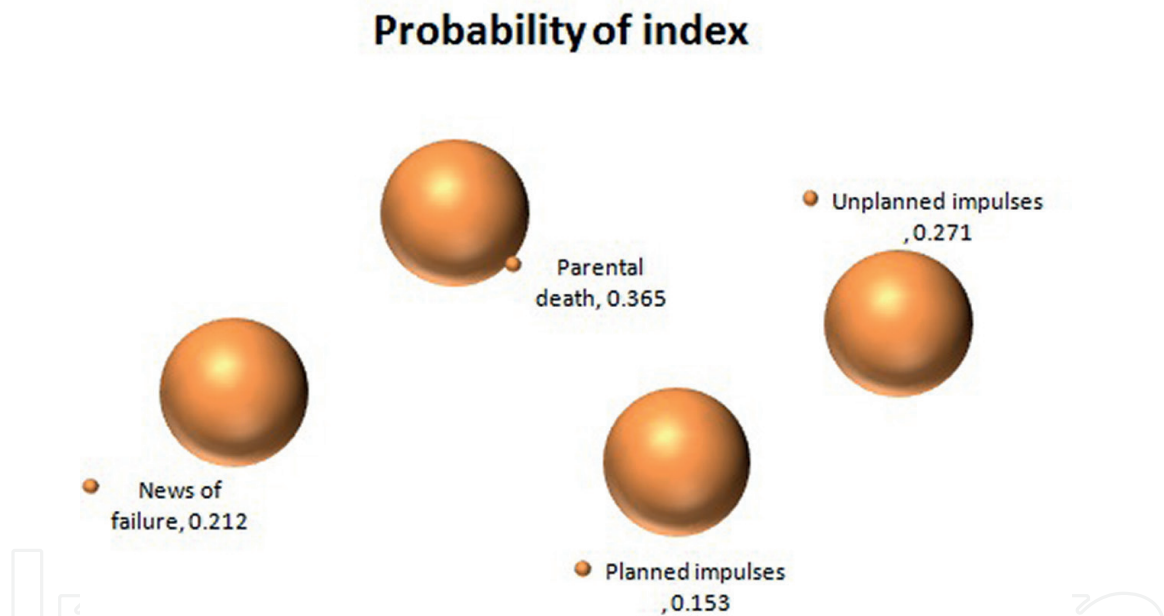


Figure 5.
 Second category of rationale that underlie the elements of juvenile crime with malware apps.

The above observations indicate that vindictive and disconsolate exhibit close statistical significance. Hence, they appear to cluster together. Conversely, failure and misfortune are not statistically close in significance. Hence, both factors appear to disperse from each other. Additionally, castaway, down grading and downcast have close statistical significance. Hence, these three factors appear to cluster together. The diagonal analysis of the variables suggest that parental death relatively aligns with news of failure as indicated by the closeness of their probabilities of occurrence. Similarly, unplanned impulses diagonally aligns with planned impulses as supported by the closeness of their probabilities of occurrence. These observations suggest that closely aligned variable can influence vulnerable children in almost the same way.

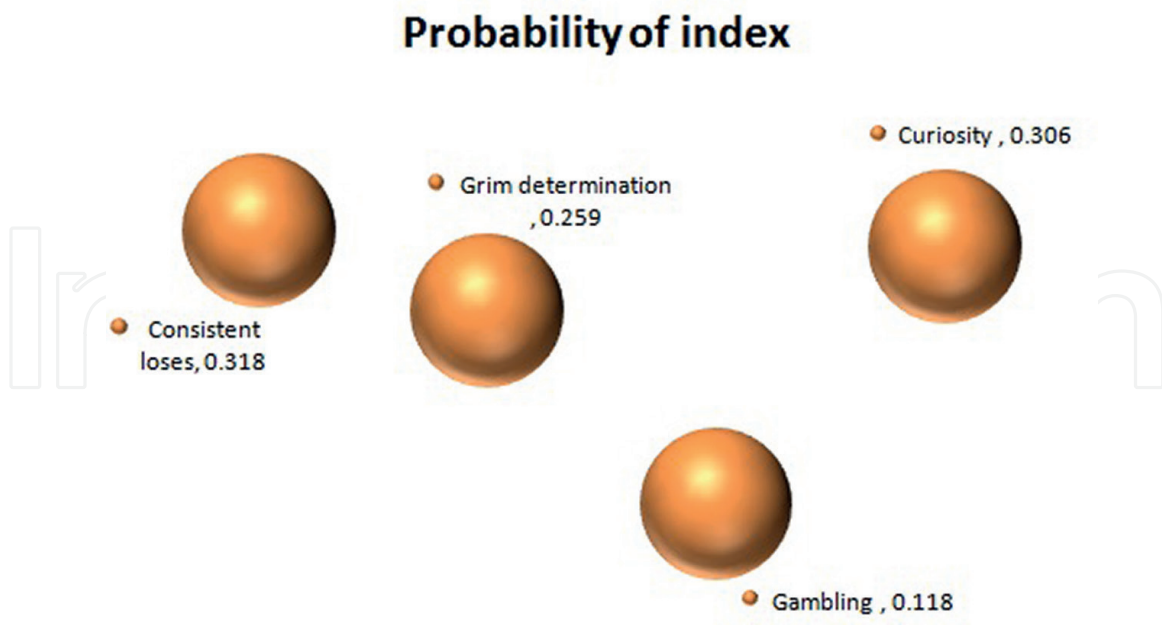


Figure 6.
Third category of rationale that underlie the elements of juvenile crime with malware apps.

Figure 6 believes that consistent loses; grim determination, curiosity and gambling are third elements of the crime that may create another group of unwholesome and objectionable circumstances for vulnerable children to be alleged of juvenile crimes with malicious apps. The results showed that consistent loses and grim determinations have close likelihood of occurrences. Hence, they appear to close to each other diagonally. In a contrast manner, gambling and curiosity are far apart because of the disparity in the likelihood of their occurrences. The diagonal analysis of these variables suggest that they do not relatively align with each other. These observations propose that grim determinations, consistent failure, gambling and curiosity can underlie the behaviour of vulnerable children in different ways.

Figure 7 establishes that bankruptcy, discontentment, disappointment and antagonism are hidden factors that underlie the fundamental elements of juvenile crimes with malware apps. The closeness in the individual probability of occurrence of the above factors connotes that they are likely to regularly compound the above issues in creating another group of unwholesome and objectionable circumstances for most of the vulnerable children to be alleged of juvenile crimes with mobile apps. The above analysis shows that anger often correlates to discontentment in some children. The above empirical experiments suggest that disappointment that comes in the form of sudden frustration whereby a child is expecting hope but consistently turn out to be hopeless expectations can induce juvenile crimes committed with malware apps. Excessive domestic violence, hostility and actions of peers, families and schools that consistently antagonizing a child can significantly lure vulnerable children to commit juvenile crimes with malware apps.

Grim determinations describe a circumstance whereby it is impossible to plea, appease or to calm down a child. Disconsolate describes a circumstance whereby a child can be sad or dejected beyond comforting such that he/she could be incapable of being consoled by fellow human being. Vindictive is a circumstance whereby a child is determined or disposed to seek for revenge, avenge or intends to seek for revenge at all cost. Bankruptcy describes the circumstance whereby a child completely or suddenly get ruined or discovers that he/she has lacked some basic, moral, spiritual and

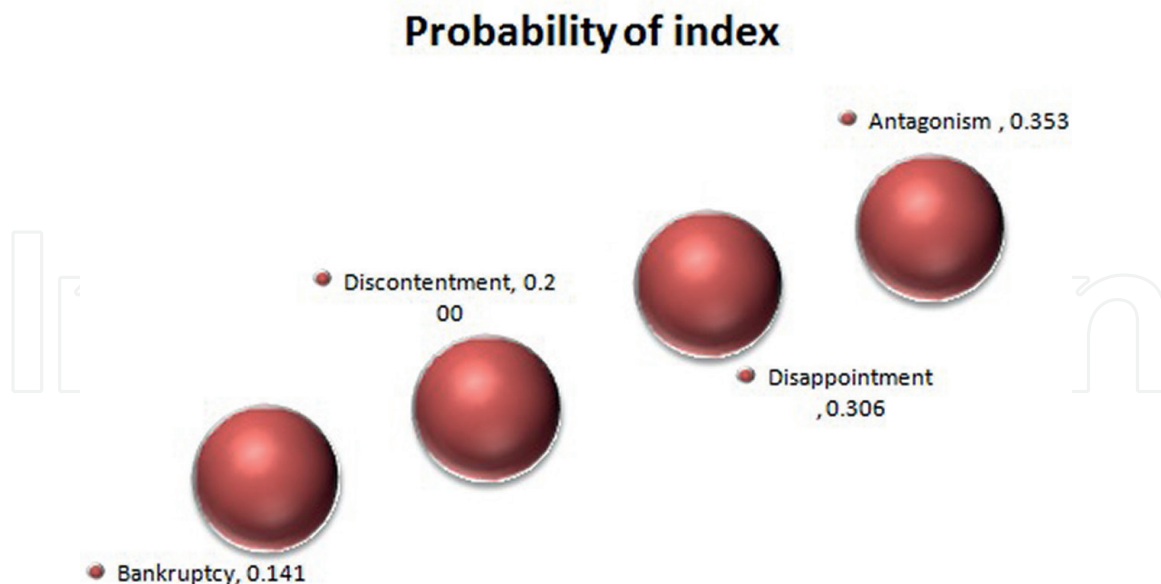


Figure 7.
Fourth category of rationale that underlie the elements of juvenile crime with malware apps.

intellectual properties that constitute wellbeing in human life [14]. Discontentment is the circumstance whereby a child is unhappy due to failure to meet up with his/her yearning desire, especially for the desire to acquire or attain something better than his or her present situation or attainment in the society.

Further still, according to the Oxford dictionary [14], disappointment is the circumstance whereby a child conceives the feeling of dissatisfaction especially if his/her expectations are not realized at the expected time. Dissatisfaction is a circumstance whereby a child is feeling of frustration or a child is being displeased (or perceives) disgruntlement with particular services, himself/herself or some things in the society. News of failure is a circumstance where a child is unable to manage sudden (or intermittent) news of consistent failure. This may occur if a vulnerable child is unable to successfully accomplish the projected height, tasks or goals in life having tried all his or her capability to accomplish the goals (tasks) on several occasions. Castaway is the circumstance whereby a child is rejected or discarded (or the child continues to feel that he/she is rejected or discarded) by his/her home and the society that he/she lives. Down grading is a circumstance whereby a child is reduced and blatantly made to appear (or continues to feel) as if he/she is an insignificant person in home and society. Down cast is a circumstance whereby a child is dejected or depressed (or the child feels that he/she is wretched) beyond immediate recovery. Misfortune is the circumstance whereby a child perceives bad luck, or the child is facing untold hardship or uncontrollable hard times. Antagonism is the circumstance whereby a child is often confronted with uncontrollable and inflexible opposition such as rigid hostility; lack of sympathy, resentment and firm hatred.

In reality, juveniles are young people that have not fully attained adulthood. They may depend on their parents, guardians or fostering cares to meet some basic requirements of daily living. They must not be abandoned so that they will not grow up with abandoned hope. Juveniles will need empathy, caring and loving people that can comfort and motivate them whenever they are contestants and whenever they suddenly stumble on obstacles (or unavoidable pitfalls) in life that can make them record sudden loses in competitions. Therefore, adequate social and restorative or

rehabilitative interventions should be specially designed for children that are affected with sudden news of failure, parental death and depression [24].

The above findings have raised about five legal and technical discussions in modern society. Suppose a juvenile crime is committed with malware apps and by means of mobile phone that involves the illegal movement of huge cash from an account of a customer into an account in another bank. This illegal cash movement obviously involves two banks. Then, who should have stopped the crime? Should we attribute the “negligence to have prevented the crime” to the two banks, telecommunication or software companies that provide banking services to both banks? Who will the victim (bank’s customer) sue in this case? Thus, the above striking observations have also called for sudden review of social policies for young children to assist parenting and policing in adequately safeguarding vulnerable children across the globe. Governments should diversify social interventions towards the various forms of the derived determinants of juvenile crimes with malware apps that are discovered above. Media involvement in the education of masses on the dangers of malware apps, unintentional cybercrimes and how innocent children may be incriminated for unknowingly committing juvenile crimes with malware apps are urgently needed in all nations of the globe. Policy makers might need to review the enabling legislations to explicate new legal issues that we raised in this chapter. In effect, software companies and service providers that market or design computer apps must thoroughly review their Service Level Agreements (SLAs) together with the underlying security functionalities of their products to accommodate new legal concepts in software industry. For instance, the issues of transfer of criminal liability, shared or joint liability, criminal consent of underaged children and the other vital issues that we have identified above demands urgent review in law books and contemporary bulletins. Government should review and direct some social interventions towards enhancing mass literacy in order to discourage youths from kleptomaniac lifestyle and excessive passion to acquire money by all means. Social interventions that will enable children to strictly adhere to the standard way of live and regulation of the level of exposure of children to some social activities (e.g. films and video) must be vigorously emphasized.

Comprehensive suit that indicate package of social interventions such as legislative protection, scholarship and financial grants to indigent children are recommended for assisting vulnerable juveniles in the above context. Governments across the globe should constantly review the existing social interventions to ensure that they are properly tailored towards the prevention of the above activities that may compel juveniles to be vindictive, disconsolate and experience unmanageable failures, misfortune, castaway, down grading and downcast in the society. Interventions should counter the negative impacts of news of failure, parental death, planned impulses and unplanned impulses and consistent loses. Juveniles require educative interventions to enlighten them on the dangers in grim determination, excessive curiosity and gambling and how they can manage unforeseen circumstances in early life. The above thoughts and paradigms are strongly recommended to counter the kinds of juvenile crimes that are studied in this chapter.

6. Conclusion and summary

This chapter has shown that malware apps are malicious apps that are strongly competing with legitimate computer apps in the software industry in recent time. It has been shown that malware apps have intrusive or criminally-minded motives that

underlie their functions, usage and practices. The motives of their designers and their users are to use them to corrupt, explore, delete, deface, swindle or steal resources or personal details of another people. Thus, we further classified prominent malware apps that are competing with legitimate computer apps in the software industry on the basis of their coaching skills. Several social and legal dilemmas came to fore in this study. The rationale that underlies the behavior of a child may be influenced by many unexpressed and unnoticeable circumstances that may initially elude the imaginations of their parents, guardians and fosters. These determinants can gradually upsurge and eventually attain high climax over time. The danger begins to increase if the affected child voluntarily or involuntarily commits juvenile crimes with malware apps against known or known victims. The influx of software industry with numerous computer apps has led to the classifications of computer apps into two groups in this chapter. Many business-oriented apps are target of malware apps that have been designed by fraudulent people.

Moreover, bankruptcy, economic failure and poverty may be inducers of juvenile crimes committed with malware apps. This study further observes that some factors such as grim determination, disconsolate, parental death, downcast, disappointment; uncertainties about future and down grading a child, etc. that underlie the fundamental elements of the above crimes have not been empirically substantiated over the years. In other words, the correlation between the elements of the crime and the circumstances that surround vulnerable children that were rarely buttressed and made explicit by empirical studies over the year have been empirically investigated in this chapter. For this reason, virtual interactions with the participants in the survey that is reported in this chapter adduce the above lapses and their correlations with the dwindling of the efficacies of several social policies in most countries. Some of the intentions of malware apps like deceptive coaching, deceptive dating guidance and fake financial coaching tips have been enumerated above. We specifically argue that malware apps can expose the users of legitimate apps and continued usage of legitimate apps to greater risk of distraction and sudden neglect if the trend of their incursion into the software industry is not quickly curtailed.

Above all, this chapter has raised novel legal debates on four vital paradigms and other technological issues concerning the legal and technical interpretations of juvenile crimes committed with malware app that urgently call for in-depth legal consideration and interpretations. We submit that malware apps with deceptive motives may send malicious files (or documents) to a vulnerable child and lure the child to download (or open) the files in order to unlock his/her internet account. The files may be Trojans or virus that will in turn corrupt other computer apps in the digital systems of the child or flout the security of another person without the consent of the child. We have therefore identified new issues regarding shared or joint criminal liability, the transfer of criminal liability, the restrictive applicability of the criminal consent of a child that is still under the tutelage and guidance of their parents and the circumstances whereby some legitimate apps may be held (or charged) by complainants for being liable to have criminally permitted some juvenile crimes that severely impact them (or to have permeated malware apps that spread virus or malicious information to propagate through them either by accidental (inadvertent, unintentional or unplanned) or intentional manner.

In addition, another dilemma that we put forward in this chapter is how the software companies and service providers can acceptably account for fake voice apps (for instance) that are proven to have adopted the data (e.g. multimedia data and textual data) they have previously gathered from vulnerable children to defraud

some people or swindle some vulnerable friends or cause controversies among the relatives of the users in the later time. We therefore raise new legal debates regarding industrial conflict and amicable resolution of disputes in relation to the procedures for compensating end-users (or paying) for the damages end-users might have incurred by virtue of “the services they receive and the confidence (or trust) they have that underlie the use of the computer apps”, especially if the damages are proven to be directly caused by the occurrence of unexpected intrusions that the manufacturers of the computer apps or service providers (vendors) should have stopped from taking place.

The premise is that the impacts of juvenile crimes with malware apps on victims must not statistically correlate to stigmatization, shame, stress, hurtful experience or increased anxiety. Otherwise, several victims of the crimes may cover up their tribulations and harms that they have incurred from the crimes. Therefore, we suggest that global governance should be directed towards the review and constant improvement of criminal laws to ensure that local and multinationals together with third party (service providers) can be effectively held to account for aiding or failing to mitigate serious juvenile crimes committed with malware apps and their variants. We also suggest that global citizens and media sector should work together to advocate and stand against all forms of discriminations against victims of the above crimes. We solidly believe that victims of juvenile crimes with malware apps require social interventions for them to recover to normal life. We recommend that future research work should delve into the above legal paradigms. Inter-disciplinary collaborations that will ensure accurate media’s representations of the methodology, prevalent and prevention of juvenile crimes that some children may commit with malware apps are inevitable in order to enlighten vulnerable children and to maximize the efficacies of the preventive and restorative interventions that governments and Non-Governmental Organizations (NGOs) have designed for the above category of global crimes.

Finally, we believe that the lists of legitimate apps and malware apps in the software industry across the globe may be inexhaustible when compare to all the computer apps that we have mentioned in this chapter. There are possibilities of fake homework coaching apps and fake fitness coaching apps. We might have only discussed malicious apps that may not comprise the entire competitors with legitimate apps in the industry. Therefore, we strongly recommend future research work to improve on the limitations of the above research findings.

IntechOpen


IntechOpen

Author details

Joshua Ojo Nehinbe
ICT Security Solutions, W/Africa

*Address all correspondence to: nehinbe@yahoo.com

IntechOpen

© 2022 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/3.0>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. 

References

- [1] Clarke-Midura J, Sun C, Pantic K. Making apps: An approach to recruiting youth to computer science. *ACM Transactions on Computing Education*. 2020;**20**(4):1-23. DOI: 10.1145/3425710
- [2] Wright JH, Mishkind M, Eells TD, Chan SR. Computer-assisted cognitive-behavior therapy and mobile apps for depression and anxiety. *Current Psychiatry Reports*. 2019;**21**:62. Available from: <https://pubmed.ncbi.nlm.nih.gov/31250242/>
- [3] Aditya K. Comparative Study of Juvenile Delinquency Law Between India, USA and UK. 2022. Available from: <https://ssrn.com/abstract=3607875> [Accessed: May 22, 2020]
- [4] Gatti U, Tremblay R, Vitaro F, McDuff P. Youth gangs, delinquency and drug use: A test of the selection, facilitation, and enhancement hypotheses. *Child Psychology and Psychiatry*. 2005;**46**(11):1178-1190. DOI: 10.1111/j.1469-7610.2005.00423.x
- [5] Davis AM. *Great Software Debates*. Wiley-IEEE Computer Society; 2004. ISBN-13: 978-0471675235
- [6] University of Minnesota. *Criminal Law: Element of Crime*. USA. Available from: <https://open.lib.umn.edu/criminallaw/chapter/4-1-criminal-elements/>; University of Minnesota; 2022 [Accessed: July 31, 2022]
- [7] Omoniyi MBI. Juvenile crimes and its Counseling implications. *Journal of Psychology*. 2011;**2**(1):1-6. DOI: 10.1080/09764224.2011.11885455
- [8] National Research Council and Institute of Medicine (NRCIM). *Juvenile crime, juvenile justice*. Panel on juvenile crime: Prevention, treatment, and control. In: McCord J, Widom CS, Crowell NA, editors. *Committee on Law and Justice and Board on Children, Youth, and Families*. Washington, DC: National Academy Press; 2001. DOI: 10.17226/9747
- [9] Eastcom C. Mathematically modelling victim selection in cyber crimes. In: *ICCWS 2021 16th International Conference on Cyber Warfare and Security*. USA: Tennessee Tech University and Oak Ridge; 2021
- [10] Wu J, Hu X, Orrick EA. The relationship between motivations for joining gangs and violent offending: A preliminary test on self-determination theory. *Victims & Offenders*. 2022;**17**(3):335-349. DOI: 10.1080/15564886.2021.1898508
- [11] Lee Y, Tae SG. A modeling perspective of juvenile crimes. *International Journal of Numerical Analysis and Modeling*. 2011;**2**(4):369-378
- [12] Oxford Dictionaries. *Crime*. 2022. Available from: <https://www.oxfordlearnersdictionaries.com/definition/english/crime?q=crime>. [Accessed: August 12, 2022]
- [13] Oxford Dictionaries. *Commission*. 2022. Available from: https://www.oxfordlearnersdictionaries.com/definition/english/commission_1?q=commission. [Accessed: August 12, 2022]
- [14] Oxford Dictionary. *Disappointment*. 2022. Available from: https://www.oxfordlearnersdictionaries.com/definition/american_english/disappointment. [Accessed: September 14, 2022]
- [15] Shamim A, Batool Z, Zafar MI, Hashmi N. A study of juvenile crimes

in Borstal jail, Faisalabad, Pakistan. *The Journal of Animal & Plant Sciences*. 2009;**19**(2):101-103

<https://study.com/academy/lesson/the-elements-of-a-crime-definition-lesson.html>. [Accessed: July 30, 2022]

[16] Young U, Greer B, Church R. *Juvenile Delinquency, Welfare, Justice and Therapeutic Interventions: A Global Perspective*. London: Cambridge University Press; 2018

[24] Jufria M, Nazerib NBM, Dhanapal S. Restorative justice: An alternative process for solving juvenile crimes in Indonesia. *Brawijaya Law Journal*. 2019;**6**(2):157-169

[17] Ellis L, Beaver K, Wright J. *Handbook of Crime Correlates*. 2nd ed. Academic Press; 2019. ISBN: 9780128044773

[18] Razzaq A, Hur A, Ahmad HF, Masood M. Cyber security: Threats, reasons, challenges, methodologies and state of the art solutions for industrial applications. In: 2013 IEEE Eleventh International Symposium on Autonomous Decentralized Systems (ISADS). 2013, 2013. pp. 1-6. DOI: 10.1109/ISADS.2013.6513420

[19] Rajib M. *Fundamentals of Software Engineering*. 5th ed. Delhi, India: PHI Learning Pvt. Ltd.; 2018

[20] Qi-qi H. Analysis on the causes of juvenile crimes from the perspective of psychology. *Academic Journal of Humanities & Social Sciences*. 2020;**3**(10):55-59. DOI: 10.25236/AJHSS.2020.031008

[21] Saylor dot org. Chapter 4 The Elements of a Crime. 2022. Available from: https://saylor dot org. github. io/ text_ criminal- law/ s08- the- elements- of- a- crime. html. [Accessed: July 30, 2022]

[22] Britannica. The Elements of Crime. 2022. Available from: <https://www. britannica. com/ topic/ criminal- law/ The- elements- of- crime>. [Accessed: July 20, 2022]

[23] Brittany McKenna Show bio. *The Elements of a Crime: Definition & Overview*. 2021. Available from: