RISK PERCEPTION AND KNOWLEDGE OF CYBERCRIME AND ITS PREVENTIVE STRATEGIES AMONG YOUTH AT THE UNIVERSITY OF BOTSWANA

Boitumelo Matlhare
University of Botswana, Department of Sociology
matlhareboi@gmail.com

Gabriel Faimau*
University of Botswana, Department of Sociology
faimaug@ub.ac.bw

Latang Sechele
University of Botswana, Department of Sociology
sechelelt@mopipi.ub.bw

Abstract

As more people invest in the cyber world, they become prone to cybercrimes. Previous studies revealed that with technological and cyber advancement, our cyberspace has been infested with malicious acts by cyber criminals while awareness and knowledge of cybercrime and related security among cyberspace users have been relatively lacking. The purpose of this study was to investigate how much knowledge the young cyberspace users at the University of Botswana (UB) have regarding cybercrime and preventive measures and strategies to fight it. Using a convenience sampling technique, data was collected from 57 female and 43 male participants. The study established that the youth at UB are aware of cybercrime, and that this awareness ranged between poor or little knowledge on cybercrime. Findings also noted low detection of cybercrime. To effectively fight cybercrime, the article recommends routine collaboration among policy makers, law enforcers, experts in both the public and private sectors, among other stakeholders.

Keywords: cybercrime, cyberspace, youth, awareness, knowledge, Botswana

1.0 Background

Botswana is a landlocked country in Southern Africa sharing borders with South Africa, Namibia, Zambia and Zimbabwe. As the country joins globalization, information age and knowledge-based economy, the use of computers and the internet becomes imperative. Growing economy requires an increase in the use of technology as more people adapt to and adopt the latest technology and fast internet. Ways of communication and lifestyle have improved due to the internet, and dependency on the use of the cyberspace has become unavoidable. However, advancements in the cyberspace now face a new type of crime which is deeply embedded within technological development and cyber use sophistication—cybercrime. Many users of the cyberspace are unaware or have very little knowledge of what cybercrime is and how it has affected the fabric of society at large (Bruijn & Janssen, 2017). While investing in information technology is the trend of our time, “it is impossible to assure information security without raising awareness among users” (Ismailova et al., 2019, p.133). The realization of a problem in a society is the first step to finding the solution.

The purpose of this research study was to investigate the extent to which youths at UB were aware of cybercrime and its preventive strategies. In particular, the study sought to determine what the youth knew about cybercrime, whether they were aware of how it happens and whether they knew about preventive strategies to guard against it.

2.0 Defining cybercrime

Cybercrime is a computer-mediated crime that revolves around the development of information and computer technology. It is a criminal activity that involves the use of a computer to perpetuate crimes in the cyberspace (Cobb, 2018). Dashora (2011) avers that cybercrime is a side product of internet development. Increase in the use of and involvement in the cyberspace has created loopholes for cyber criminal activities. Scholars have generalized the definition of cybercrime as the unlawful acts where a computer may be used as a tool in activities such as cyber defamation, cyber stalking, intellectual property theft, online gambling, child pornography and fraud. Others argue that cybercrime does not only involve the use of a computer as cyber criminals can also use human efforts such as dumpster diving to search for paper documents, disk drives and automated teller machine (ATM) receipts to harvest information to use for hacking (Ba, 2017; Virtanen, 2017; Cobb, 2018). Cybercrime thus relates to a computer, a network, and/or information technology.

Cybercrime has dominant unique features that make it stand out from other types of crime, and which have it hard for law enforcement agents in various countries to fight it (Chimuka & Mashumba, 2016). First, cybercrime is an international borderless crime, and this decreases chances of cyber criminals getting caught because they do not have to be there physically to commit the crime (Sarre, Lau & Chang, 2018). With a human trafficking syndicate, the human smuggler might get caught between borders of countries, but it might be before the smauggler is apprehended. However, electronic hacking can be done successfully within minutes, and to apprehend the perpetrator would require investigations that could stretch into months or more. Additionally, cybercrime involves a high technological threshold, indicating remarkable skill in computer technology by cyber criminals and ability to hide digital footprint. Cyber police would thus need to have exceptional skills in computer technology to be able to detect cybercrime and trace the ‘hidden’ digital footprints. High technological awareness also becomes imperative (Nouh, Nurse, Webb & Goldsmith, 2019). Anonymity is a strong feature of cybercrime (Ba, 2017). The cyberspace on its own creates a platform for effortless camouflaging of cyber criminals, which is a challenge when trying to identity the perpetrators. One other feature of cybercrime is that it is an orchestrated crime which involves careful planning and careful making of vigilant decisions (Virtanen, 2017; eSilva, 2018).

3.0 Cybercrime in Botswana

Botswana has steadily registered a high percentage of internet users among its population of two million. As of 2019, the country registered a total of 1,997,322 mobile internet and fixed internet subscriptions (Statistics Botswana, 2019). This number shows an increase of 10.7 percent from the total 1,804,449 subscriptions in 2018. Mobile internet has registered more subscriptions compared to fixed internet subscriptions over the years. With relatively high percentage of and ever increasing internet usage, the possibility of cybercrime activities cannot be avoided. While comprehensive study on cybercrime cases in Botswana is certainly required, in 2017 the African Union Commision declared Botswana the most cyber attacked country in the continent. Consequently, Botswana was labeled the cybercrime capital of Africa (*Sunday Standard*, 2017). The then Botswana Police Service spokesperson, Senior Superintendent Near Bagali indicated that Botswana is no stranger to cybercrime as the Police offices countrywide have been snowed under with reports of companies and individuals who were victims of cyber-facilated crimes (Tebele, 2018). Senior Superintendent Bagali further expressed that the reason for high cybercrime rates was because of an increase in the use of internet and social media, especially in the capital city Gaborone. Other reports have similarly shown that in 2016, a total of 37,889 cyber attacks originated from Botswana, which accounted for three percent of all cyber attacks in the continent of Africa (Tebele, 2018).

Botswana is an import based economy and relies on goods and services from other coutries. This makes it a potential haven for cyber criminals. Investors such as Huawei, an international Information and Communications Technology (ICT) provider, have warned Botswana companies to take measures against cybercrime (Maramwidze, 2015), because preponderance of this type of crime could lead to investors losing large amounts of money. Heeding such warning is crtical because cybercrime is a threat not only to national but to international security as well. Encouraging signs that the warning is being heeded is that some institutions are taking precautionary steps to guard against cybercrome. For instance Bank Gaborone took an initiative to caution its customers after they received fraudulent emails allegedly from the bank (Maramwidze, 2015). Although reports on cybercrime are quite low compared to conventional crimes such as rape or robbery, the nature and speed with which this type of crime can be committed, among others, indicate that it should not be taken lightly. Strict measure should be put in place to tighten cyber security in the country.

4.0 Policies relating to cybercrime in Botswana

To address the threat to national and international security posed by cybercrime in Botswana, several policies and laws have been developed. The first policy named Maitlamo National Information Commucation Technology addressed issues pertaining to ICT in general.

Maitlamo policy was established in 2004 with the mandate to ensure that Botswana became a universally competitive, knowledge and information society where developments in social, economic and cultural sectors were achieved through effective use of ICT (Republic of Botswana, 2004). The objectives of the policy include forming an environment that encourages growth of the ICT industry, providing extensive access to fast internet, fast information and fast communication, and turning Botswana into a regional hub to promote global competitiveness.

Increase in the use of ICT necessitated the development of other laws to strengthen security against cybercrime. In 2007, the Cybercrime and Computer-related Crimes Act was first passed in parliament. The Act aimed at curbing criminal activities committed through computers and also facilitated the collection of electronic evidence. Acknowledging the importance and the urgency of responding to cybercrime and computer-related crimes, the 2007 Act was later amended and modernized in 2018. The Act was named Cybercrime and Computer-related Crimes Act 2018. The amendment of the 2007 Act was a response to a great need for having a modernized Act with more detailed and precise description of cyber-related crimes to make sure it was on par with other international cybercrime laws. Also, in 2018 legislation focusing on data protection was formed. Granted and approved by Botswana Parliament on 3 August 2018, the Data Protection Act (DPA) was created solely for the protection of personal data; and the Act further provided and meticulous definition of the principles of data processing. In this Act, personal data refers to information that can be directly or indirectly related to an identified or identifiable individual, with particular reference to their ID number or social identity. The Act also states that personal data should only be processed lawfully, transparently, and fairly (Kelly, 2018).

Much like the Data Protection Act 2018, confidentiality of data, right to accesses, duty of data controller, integrity of computer systems and gathering of electronic evidence are objectives of the Cybercrime and Computer-Related Crimes Act 2018. When the Act was passed by the parliament, the then Minister of Defense, Justice and Security, Honourable Shaw Kgathi, informed the public in an interview that the Act was amended to keep up with the new crimes arising from the use of cyberspace, such as cyber-terrorism, money laundering, trafficking of illegal and harmful chemicals, cyber-stalking, cyber-harassment as well as revenge pornography (Tebele, 2018). The Act was also amended to provide law enforcement officers with procedural powers over cases of cybercrime.

5.0 Statement of the problem

Acute concern surrounding cybercrime and cybersecurity among internet users contribute towards lowing the risks of cybercrime (Bruijn & Janssen, 2017). The state has the responsibility of protecting information and information systems in the interest of citizens. Botswana has taken measures to address the problem of cybercrime by developing policies and laws such as the Cybercrime and Computer-Related Crimes Act of 2007 and the 2018 Data Protection Act. For these laws to be effective, there must be a fundamental understanding and knowledge of cybercrime, and a critical change in attitudes towards it from the general public. Batane (2013) discovered that the youth in Botswana are the group most connected to the internet. With the increasing number of internet use among the youth in Botswana, it remains to be seen how much awareness and knowledge of cybercrime these members of the community have. The purpose of this study was thus to examine the awareness and knowledge of cybercrime and preventive measures against it among the youth, with particular focus on the youth at UB.

6.0 Perspectives on cybercrime

In recent years, there has been a growing interest in scholarly studies on cybercrime. This section provides some perspectives on cybercrime and covers the following key issues: common types of cybercrime, the risky perception of cybercrime and challenges affecting law enforcement in Botswana in regard to cybercrime.

6.1 Common types of cybercrimes affecting youth

The internet allows for various cybercrimes such as identity theft and cyberbullying to occur. The borderless aspect of cybercrime further takes this to higher level in facilitating the spread. Anybody can be a victim, including business organizations, the state and general users of the cyberspace. Organized cybercrimes such money laundering, cyber terrorism, and human trafficking are usually orchestrated by organized criminals, while cybercrimes such as cyberstalking and revenge pornography are done by individuals behind the computer or on their cell phones in the comfort of their own homes. With people spending a lot of time on their mobile phones and computers, it is inevitable that they would upload personal data on the internet and thus expose themselves to the possibility of a crime such as identity theft. Identity theft is a form of cybercrime that entails stealing another person's identity (Dashora, 2011; Weijer, Leukfeldt & Bernasco, 2019). A newspaper report published in 2008 cited the then Detective Superintendent Balibadzi Boy of Naledi Police Station in Gaborone confirming that there had been frequent cases of identity theft in the country in and prior to 2008 (Pitse, 2008). The same newspaper report stated that 14 medical doctors based in Princess Marina Referral Hospital had part of their salaries fraudulently deducted from their personal accounts in an insurance identity theft case. The number of cybercrime cases has since been steadily increasing in the past decade (Adamson, 2018). Identity theft also occurs on social media platforms such as Facebook where cyber criminals can collect personal data from their victims and create fake profiles for malicious activities (*Sunday Standard*, 2014).

Cyber-bullying is another global challenge. Bullying is referred to as the aggressive, intimidation and the oppression of a vulnerable and defenceless victim. Cyber-bullying refers to the same thing, with the exception that it happens online, behind a phone or a computer connected to the internet (Li, 2010; Dashora, 2011; Tezer, 2017). Cyber-bullying involves posting embarrassing pictures of the victim, harassing, threatening, and tarnishing another person's name online. Botswana Communications Regulatory Authority (BOCRA) has warned the public to be vigilant and stop normalizing cyber-bullying (Tebele, 2018).

Furthermore, the youth in particular are also faced with phishing. Phishing is when cyber criminals make attempts to trick potential victims into revealing critical personal data such as bank accounts (Tebele, 2018).

6.2 The risky perception of cybercrime by internet users

As indicated above, cybercrime is growing at a startling rate, and reasons being increased use of the cyberspace accompanied by lack of awareness of lurking dangers. At global level, reports state that in 2019 the most targeted sectors of cybercrime are professional and public services, with 7,463 and 6,843 incidents respectively (Clement, 2020). Statistical data on cybercrime indicate that in 2017, federal agencies in the United States received 35,227 reports relating to cyber security incidents (Clement, 2019). Between 2011 and 2015, India had recorded over 32,000 cybercrime incidents (Pradeep & Arjun, 2018). A National Computer Security Survey (NCSS) conducted by the US Bereau of Justice Statistics found that in 2005, more than 60 percent of 7,818 businesses detected at least one cybercrime and one or more types of cyber attack. The same survey revealed that among the businesses involved in the study, 11 percent detected cyber thefts and 24 percent experienced other computer security incidents. Cybercrime is also costly as the survey additionally showed that 3,247 businesses lost a total of $867 million from cybercrime in 2005 (Rantala, 2008; Bureau of Justice Statistics, n.d.). Based on the current cybercrime trends, Cybersecurity Ventures in its 2019 report predicted that “cybercrime will cost the world in excess of $6 trillion annually by 2021, up from $3 trillion in 2015” (Morgan, 2019, p. 2).

6.3 Cybercrime and challenges of law enforcement in Botswana

Chimuka and Mashumba (2016) demonstrate the difficulties of enforcing cyber laws in the country. Firstly, there is a huge digital divide and little expertise surounding law enforcement officials. For instance, the qualification needed for recruitment of Special Constables in the Botswana Police Service (BPS) as is a secondary education with at least 30 points, with Grade C or better in English language. After recruitment, the Constables are primarily trained to fight visible, physical, enviroment crimes and are hardly ever trained to confront cybercrimes. This situation needs to be rectfied considering that the Police are gatekeepers of a comprehensive, all encompassing criminal justice system, and are the people to go to when one has been violated in any way. Since (cyber) criminals are usually ahead of law enforcers, there is a dire need for revised cybercrime frameworks which will require police officers to be trained to detect and address cybercrime as much as they confront other types of crime. Chimuka and Mashumba (2016) also noted unsophisticated technology in the criminal justice system as a serious drawback. There is limited capacity to adeqautely deal with cybercrime by the police, which influences how investigations are done, resulting in poor collection of evidence. Furthermore, Botswana has an undersized Police Information Technology Unit which is responsible for the collection and preservation of electronic evidence for court. Its main challenge has been the presentation of evidence in court because the court systems is not developed enough to receive improved and quality evidence. Electonic screens and the use of computers to allow visually presentation of evidence are some of the lacking facilities (Chimuka & Mashumba, 2016).

7.0 A brief review of related literature

Awareness and risky perception of cybercrime has been an area of interest among scholars. Pradeep and Arjun (2018) reported that over 20 percent of 300 young people in Udupi district in India were not aware of the dangers of cybercrime such as copyright violation, deep web crimes and mobile hackings although they were active internet users. In particular, the participants acknowledged the lack of survelliance and protection on their electronic appliances. Sreehari and Abinanth (2018) conducted research based on alertness of cybercrime among 200 college students aged between 18 and 25 years in Kochi, India. Their study found that 86 percent of the respondents spent their time using the internet mostly on social media applications such as facebook, twitter, and instagam, while 94.2 percent downloaded a number of various internet content including online trading businesses. Such online activities means participants save personal details on the internet such as bank details (for buying or selling online) as well as their locations. This automatically makes them potential targets (Dashora, 2011; Weijer, Leukfeldt & Bernasco, 2019). Sreehari and Abinanth (2018) further revealed that young people do not adhere to ethical regulations once on cyberspace. One essential ethical regulation is that internet rights, personal data, and property of others ought to be respected at all times. Behaving ethically includes key pinciples such as having respect for one's online presence and data.

Sreehari and Abinanth (2018) reported further on the cybercrime awareness and safety precautions. About 25 percent of the participants said that they were aware of what cybercrime is, while 51.7 percent stated that they just knew about cybercrime. The researched opined that young people are unbothered and are not conscious about the dangers of the cyberspace; further that this could be suggestive of the fact that half of the participants would not know if they had been victims of cybercrime. Participants were asked whether or not they feel safe about leaving personal details online. Over four percent indicated that leaving personal details online and open to the public was safe, while 20.7 percent were comfortable leaving personal details online but without it being open to the public. Astonishingly, half of the respondents admitted that they had no idea whether information online was protected or not. Evidently, these users are for the most part unaware of the risks that come with using the cyberspace. On the brighter side, the study found that 71.8 percent of the students in Kochi knew about virus attacks in the cyber world.

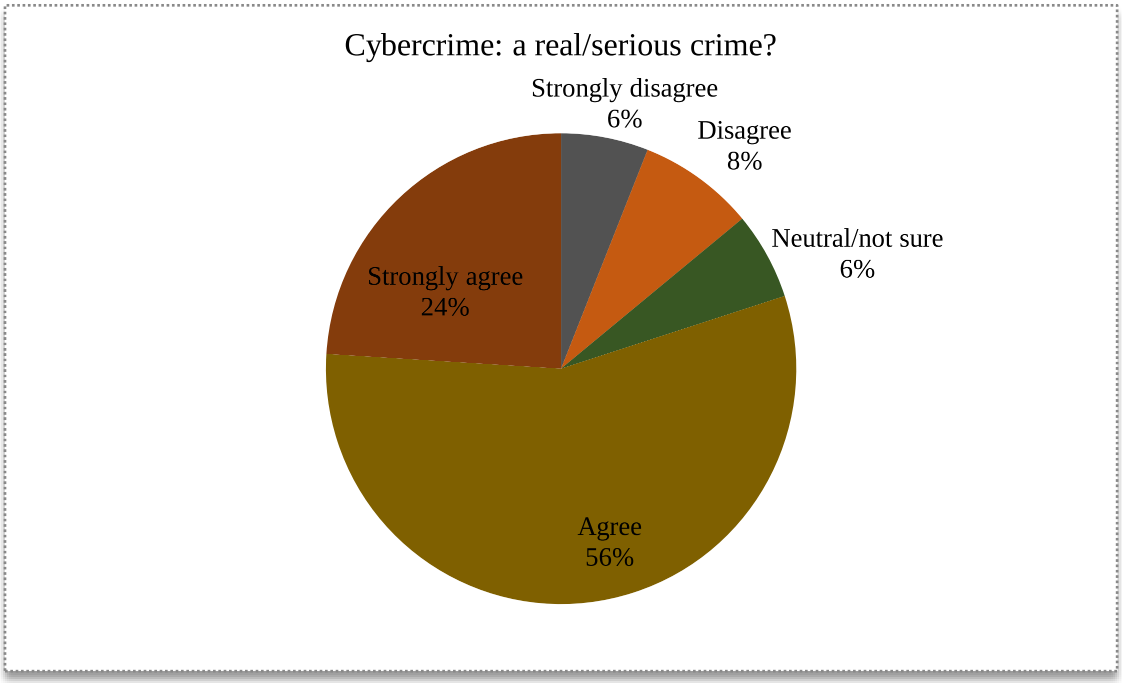
8.0 Methodology and participants

The current study was conducted between March and April 2019. The target population for this research was the youth at UB. The 2016/2017 annual report of the University showed that UB had a total of 15,146 students across different faculties and various programs of study (University of Botswana, 2017). One hundred participants were conveniently selected to participate in the study. The sample size was relatively small as the focus was to examine awareness and knowledge of cybercrime and preventive measures against it among the youth at UB as well as a meaningful understanding of the risky perception of this type of crime among the participants. In this study, youth included students and employees of UB who were between 18 and 35 years, and majority of participants were females at 57 percent. Males stood at 43 percent. The most dominant age group was between 18 and 22 years (52 percent). The students were a majority at 82 percent, while 18 participants were academic and support staff. The study adopted a quantitative approach and collected data by means of a structured questionnaire.

9.0 Analysis of data and findings

To establish the level of awareness on and knowledge about cybercrime, frequency and descriptive statistical analysis was done. Figure 1 shows that out of a total of 100 participants, 80 percent viewed cybercrime as a real crime, just like murder or rape. They also thought it was a threat to the cyberworld. Six percent of the participants were not sure whether to consider cybercrime as a real crime or not. Fourteen percent disagreed with the idea of categorizing cybercrime as a real crime. Data clearly showed that majority of participants (80 percent) recognized cybercrime as a real crime.

Figure 1: Knowledge of cybercrime as a real/serious crime

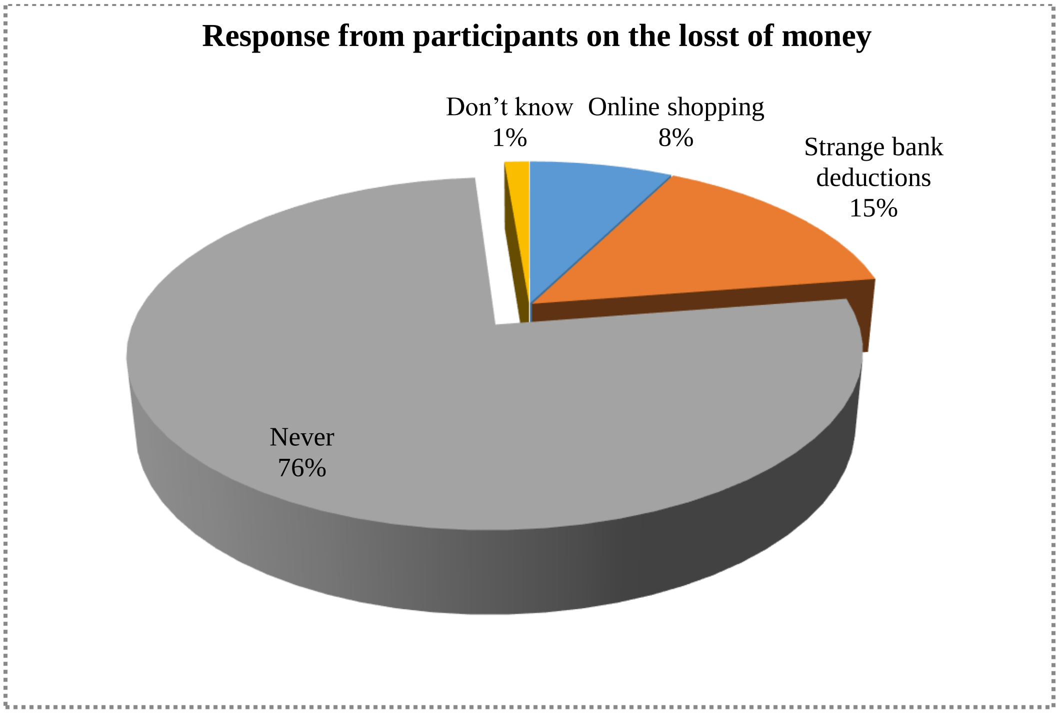


Further, out of 100 participants, 27 percent agreed and strongly agreed that being safe online was of paramount importance. On the other hand, 42 percent were not sure whether or not it was safe to be online. Thirty one percent of the respondents disagreed that it was not (always) safe to be online. Participants nonetheless showed that they take several precaution measures such as antivirus installations and change of passwords to guide against virus attacks and cybercrimes. For example, 73 percent indicated that they had antivirus software in their electronic devices, while 27 percent said they did not. Most of the participants (78 percent) strongly agreed and agreed that there was little detection of cybercrime, which was attributed to lack of knowledge about cybercrime.

The results of the study also showed that participants were aware of the following cybercrimes: cyber bullying, identity theft, phishing, hacking, cyberstalking and cyber fraud. Out of 100 respondents, 20 percent disclosed that they had been victims of cybercrime, while 23 percent were unsure, and 57 percent indicated that they had never experienced cybercrime.

Internet users generally have financial transactions occurring in the cyber space. As such, some are bound to fall victim in this kind of space. When questioned whether they had lost money online, 71 percent of the youths said they did not have that experience. Figure 2 shows the responses regarding the loss of money online.

Figure 2: Awareness of losing money online



When asked whether they had ever experienced any type of cybercrime, more than 50 percent of the participants said they had never experienced cybercrime. While only four percent of the study participants said they had been cyber-bullied, hacking and cyber-stalking were cited as the two major cybercrimes at 32 percent. Table 1 shows the types of cybercrimes that the youth at UB experienced. As depicted in Table 1, the most common cybercrimes experienced by the participants involved cyber-stalking and hacking as the study revealed that 13 percent and 19 percent of respondents experienced cyberstalking and hacking respectively.

Table 1: Types of cybercrime experienced by the youth at UB

Type of cybercrime	Percentage
Cyber bullying	4
Identity theft	6
Phishing	3
Hacking	19
Cyber stalking	13
No experience at all	55

The last section of the questionnaire was on law enforcement efforts on cybercrime. Ninety-seven of the participants claimed that they had never reported a cybercrime. Responding to the question relating to willingness to report cybercrime, 64 percent of the participants stated that they would report it. Table 2 shows responses on whether or not respondents would ever report a cybercrime. It is quite possible that 13 percent of respondents who said they would not report a cybercrime because it was not exactly a serious crime could be among the 14 percent that strongly disagreed and disagreed that cybercrime is a real crime, as already explained earlier. Two percent did not attempt to answer this question. Regarding awareness of cyber laws in Botswana, 28 percent of the participants reported knowing about them, while the rest said that they were not aware of them.

Table 2: Willingness by UB youths to report cybercrime

Would you report a cybercrime?	Frequency
Yes	64
Not sure, it is not really a serious crime	13
No, because police will not do anything about it	21
Not attempted	2

Believing in the capabilities of policies and cyber laws in combating crime is a key factor in the fight against cybercrime. The study found that 50 percent of the participants were unsure about the capabilities of cyber laws in combating cybercrime. Furthermore, data from the study suggests that 17 percent of the participants did not believe in the policies developed to deter cyber criminals from committing cybercrime. However, 33 percent of the participants believed that policies against cybercrime in Botswana are capable of combating cybercrime. What is disturbing however, is the high percentage (50 percent) of those who were unsure about the capability of the policies in combating crime. When participants were asked whether they think the police had the right technical personnel, 52 percent strongly disagreed and disagreed, and 15 percent either agreed or strongly agreed that the police had the right technical personnel. Thirty three percent were neutral on this particular question.

Participants were further asked if they would get into a police station and report any kind of cybercrime the same way they would report conventional cases. Sixty four percent of the participants quickly reported that they would, while 15 percent indicated that they were not entirely sure because cybercrime is not a serious crime. Interestingly, responding to the same question, 21 percent of the respondents suggested that there is no chance they would report cybercrime the same way they would report conventional crimes.

9.0 Discussion

This study indicated that the majority of the youth at UB were aware of cybercrime and consider it a real crime. Eighty percent of the participants of this study agreed that cybercrime was a serious crime. This level of awareness of cybercrime differs with some previous research which reported that internet users, especially the youth, knew very little about cybercrime (Dashora, 2011). Ismailova et al. (2019) and Pradeep and Arjun (2018) also noted that awareness of information security was extremely low among the youth. Sreehari and Abinanth (2018) said that a quarter of their participants were aware of cybercrime while 51.7 percent knew *about* it. However, although knowledge and awareness of cybercrime was noted to be high among the youth at UB, this study did not explore the depth of this knowledge among the participants. Bruijn and Janssen (2017) also argue that although cyber users may be aware of or at least know about cybercrime, they typically do not have much grasp the profundity and depth of this type of crime. It could be suggested that the youth at UB are only minimally concerned with cybercrime as 73 percent said they have antivirus softwares installed in their computers and frequently change their passwords. Other than that they did not put up any meaures to combat other types of cybercrime. Thus the threats of cybercrime in the global community do not seem to be a concern among the participants.

The study further revealed that 42 percent of participants were non-aligned when asked whether it was safe to be online or not. Of the 80 participants who said cybercrime was a real crime, half were not sure as to whether to be online was or was not safe. This concurs with the misconception that cybercrime is only a technical problem (Virtanen, 2017; Sreehari & Abinanth, 2018), leading to a cavalier attitude in cybersecurity. It is apparent that cyberspace users do not have a substantive and profound knowledge on cybercrime to take distinctive, firm measures with regard to safety issues on this type of platform. As a result, these ‘digital natives’ make next to no effort to be extra vigilant, strategic and smart as they need to be (Dashora, 2011; Metallo & Agrifoglio, 2015). Such measure include continuous change of passwords to ensure they are unapparent and not easy to crack. Passwords such as personal names, and birth dates are what hackers usually work with to break into the cyber world. Although 73 percent of the youths said they take some precautionary measures, it is still a concern that 22 percent did not, especially since the University as an institution of higher learning requires extensive use of the internet. Cyber criminals are able to pick up the stagnent absence of cyber security.

Because of the complexity of cybercrime, it is complicated to determine whether one has been a victim or not. Further, since cybercrime is not a physical crime, detection of cyber-attacks remains a considerable challenge. The physical invincibility of cybercrime makes it hard to notice any violations in the cyber space (Sharma, Ghisingh & Ramdinmawii, 2014; Viertanen, 2017; Sarre, Lau & Chang, 2018). Therefore, although 75 percent of participants in this study reported that they had never lost money online, this needs to be considered in the light of the physical complexity of cybercrimes. Furthermore, it would be difficult for cyber users to track down their financial activities without the help of technical expertise, meaning that cyber users may not even be aware that they have been victims of fraudulent activities in the cyber world.

As already indicated, 28 percent of the participants in this investigation indicated that they were familiar with the laws on cybercrime and they believe these Acts are capable of combating cybercrime. Interestingly, it was observed that being familiar with the laws and believing in their capability to combat cybercrime did not translate to victims of cybercrime easily reporting the crimes. Such findings were also noted in previous studies that reported reluctance to report cybercrimes because of the belief that law enforcers would not be able to help (Weijer, Leukfeldt & Bernasco, 2019). Law enforcement agencies need to recognise this loophole, and make effort to be seen to be actively combating cybercrime in order to gain public confidence. The police should be seen to be prioritizing cybercrimes as much as they do other types of crime (Wexler, 2014; Leppanen & Kankaanranta, 2017). The general attitude of the police in Botswana has been that if one has not experienced cybercrime, then there is nothing forcing them to investigate the crime. The Police Department needs to realize that it too has a role/contribution in winning the battle against cybercrime. They need to recognize that it is a crime to be investigated just like other types of crimes; they further need to equip themselves with the necessary knowledge and skills to tackle it effectively (Wexler, 2014; Leppanen & Kankaanranta, 2017).

10.0 Conclusion

Cybercrime is a very serious threat to individual partakers of the cyberspace, and to national and international security. Public awareness on a problem helps with the detection of the problem and with finding te solution. This study has shown that most youth at UB have an idea of what cybercrime is and of some preventive strategies against it. The level of awareness on the issue of cybercrime by the youth at UB was fairly substantial as most participants were aware of it and believed that it was a real crime. Additionaly, the findings revealed that they were aware of policies and laws in place to fight cybercrime. It is however alarming that majority of the participants did not practise extensive self-protection from cybercrime. The study recommends routine collaborations among policy makers, law enforcers, experts in both the public and private sectors, the youth and the general public to fight cybercrime. This includes applying a broad-strategy that underlines the importance of public awareness and knowledge of the nature, scale, sophistication and impact of cybercrime and other computer-related crimes.

References

Adamson, K. (2018, July 6). Over P1.6 billion stolen online. *The Patriot on Sunday*. Retrieved from https://www.thepatriot.co.bw/business/item/5756-over-p1-6-billion-stolen-online.html

Ba, Y. (2017). *Understanding cybercrime and developing a monitoring device* (Bachelor's Thesis). Turku University of Applied Sciences, Turku, Finland.

Batane, T. (2013). Internet access and use among young people in Botswana. *International Journal of Information and Education Technology, 3*(1)*,* 117-119.

Bureau of Justice Statistics. (n.d.). Cybercrime. Retrieved from https://www.bjs.gov/index.cfm ?ty=tp&tid=41

Bruijn, H.D., & Janssen, M. (2017). Building cybersecurity awareness: The need for evidence-based framing strategies. *Government Information Quarterly*, *34*(1), 1-7.

Chimuka, T.A., & Mashumba, L. (2016). Understanding cyber scams: An assessment of the challenges of law enforcement in Botswana. *Journal of Sustainable Development in Africa*, *18*(2), 111-126.

Clement, J. (2020). Cybercrime incidents worldwide 2019 by victim industry and size. Retrieved from https://www.statista.com/statistics/194246/cyber-crime-incidents-victim-industry-size/

Clement, J. (2019). U.S. government and cybercrime: Statistics and facts. Retrieved from https://www.statista.com/statistics/194246/cyber-crime-incidents-victim-industry-size/

Cobb, S. (2018). Why ask the public about cybercrime and cybersecurity? Retrieved from https://www.welivesecurity.com/2018/10/04/ask-public-cybercrime-cybersecurity/

Dashora, K. (2011). Cybercrime in the society: Problems and preventions. *Journal of Alternative Perspectives in the Social Sciences*, *3*(1), 240-259.

eSilva, K.K. (2018). Vigilantism and cooperative criminal justice: Is there a place for cybersecurity vigilantes in cybercrime fighting? *International Review of Law, Computers and Technology*, *32*(1), 21-36.

Ismailova, R., Muhametjanova, G., Medeni, T.D., Medeni, I.T., Soylu, D. & Dossymbekuly, O.A. (2019). Cybercrime risk awareness rate among students in Central Asia: A comparative study in Kyrgyzstan and Kazakhstan. *Information Security Journal: A Global Perspective*, *28*(4-5), 127-135.

Kelly, M. (2018). Data Protection Act 101: What you need to know. Retrieved from https://minchinkelly-bw.com/2018/10/15/data-protection-act-101-what-you-need-to-know/

Leppanen, A. & Kankaanranta, T. (2017). Cybercrime investigation in Finland. *Journal of Scandinavian Studies in Criminology and Crime Prevention*, *18*(2), 157-175.

Li, Q. (2010). Cyberbullying in high schools: A Study of students' behaviours and beliefs about this new phenomenon. *Journal of Aggression, Maltreatment and Trauma*, *19*(4), 372-392.

Maramwidze, A. (2015). Huawei security warning to Botswana. Retrieved from http://www.itwebafrica.com/security/636-botswana/234448-huaweis-security-warning-to-corporate-botswana

Metallo, C., & Agrifoglio, R. (2015). The effects of generational differences on use continuance of twitter: An investigation of digital natives and digital immigrants. *Behaviour & Information Technology, 34*(9), 869-881.

Morgan, S. (2019). *2019 official annual cybercrime report*. Toronto: Herjavec Group.

Nouh, M., Nurse, J.R.C., Webb, H., & Goldsmith, M. (2019). Cybercrime investigators are users too! Understanding the socio-technical challenges faced by law enforcement. *Proceedings of the 2019 Workshop on Usable Security (USEC)* (pp. 1-11). Reston: Internet Society.

Pitse, R. (2008, September 21). Identity theft rocks Botswana insurance industry. *Sunday Standard*. Retrieved from http://www.sundaystandard.info/identity-theft-rocks-botswana-insurance-industry.

Pradeep, L.M.P., & Arjun, M. (2018). Cybercrime awareness among youth in Udapi District. *Journal of Forensic Sciences and Criminal Investigation, 8*(5), 1-4.

Rantala, R.R. (2008). Cybercrime against businesses, 2005. *Bureau of Justice Statistics Special Report NCJ 221943*. Retrieved from https://www.bjs.gov/content/pub/pdf/cb05.pdf

Republic of Botswana. (2004). *Maitlamo: Botswana national ICT policy*. Gaborone: Government Printers.

Sarre, R., Lau, L.Y., & Chang, L.Y.C. (2018). Responding to cybercrime: Current trends. *Police Practice and Research: An International Journal*, *19*(6), 515-518.

Sharma, U., Ghisingh, S., & Ramdinmawii, E. (2014). A Study on the Cyber-Crime and Cyber Criminals: A Global Problem. *International Journal of Web Technology*, *3,* 172-179.

Sreehari, A., & Abinanth, K. (2018). A study of awareness of cybercrime among college students with special reference to Kochi. *International Journal of Pure and Applied Mathematics*, *119*, 353-1360.

Statistics Botswana. (2019). *Information communication technology stats brief*. Gaborone: Government Printers.

Sunday Standard. (2014, March 02). Exploring identity theft. *Sunday Standard Newspaper*. Retrieved from https://www.sundaystandard.info/exploring-identity-theft/.

Sunday Standard. (2017 August 28). Botswana is the cybercrime capital of Africa. *Sunday Standard Newspaper*. Retrieved from https://www.sundaystandard.info/botswana-is-the-cyber-crime-capital-of-africa/.

Tebele, M. (2018, July 02). Botswana businesses hit by cybercrime. Retrieved from https://southerntimesafrica.com/site/news/botswana-businesses-hit-by-cybercrime.

Tezer, M. (2017). Cyber bullying and university students: Behaviours, opinions, and reactions. *International Journal of Educational Sciences*, *19*(2-3), 199-204.

University of Botswana. (2017). *University of Botswana Annual Report 2016/2017*. Retrieved from https://www.ub.bw/sites/default/files/2018-06/UB-AR-201617.pdf

Virtanen, S.M. (2017). Fear of cybercrime in Europe: Examining the effects of victimization and vulnerabilities. *Psychiatry, Psychology and Law*, *24*(3), 323-338.

Weijer, S. G. van de, Leukfeldt, R., & Bernasco, W. (2019). Determinants of reporting cybercrime: A comparison between identity theft, consumer fraud, and hacking. *European Journal of Criminology*, *16*(4), 486-508.

Wexler, C. (2014). *The role of local law enforcement agencies in preventing and investigating cybercrime.* Washington D.C: Police Executive Research Forum.