ISSN: 2996-3397

Research Article

International Journal of Criminology and Criminal Law

Cybercrime on the Socio-Religious Lives of Muslim Youths

Abdul Aziz Shamhuna*

Religious Studies Department, Islamic University College, Ghana

***Corresponding Author**
Abdul Aziz Shamhuna, Religious Studies Department, Islamic University College, Ghana.

Submitted: 2025, Sep 30; **Accepted:** 2025, Nov 06; **Published:** 2025, Nov 17

Citation: Shamhuna, A.A. (2025). Cybercrime on the Socio-Religious Lives of Muslim Youths *Int J Criminol Criminal Law, 3*(4), 01-08.

Abstract

The internet is a source of mass communication all over the world. Cybercrime is the most complicated and latest problem in the cyber world. The purpose of this article is to determine, Islam and Crime, The Holy Quran and Sunnah, Prevention of Cybercrime in the Holy Quran. The article again outlines briefly, Access to Internet, Purpose of using internet, Own social media account, Meaning of Cybercrime, Types of Cybercrime among Muslim Youth, Reasons of Cybercrime, Causes of Cybercrime and Impact of Cybercrime. Qualitative methodology is adopted to determine the purpose of the article for primary data and secondary data. A number of respondents were selected. The findings disclose that majority of respondents don't know the correct definition of cybercrime and they are not even aware about the laws and punishments for cyber criminals set by the state. Results also indicates that majority of respondent's care about the religious values and they don't misuse others' private information. Laws and punishments are discussed and offered some suggestions by the researcher.

Keywords: *Cybercrime, Hacking, Cyber warfare, Crime, Internet, Cyber criminals.*

1. Introduction

A normal crime or an illegal or anti-social act is typically organized based on internet, mobile or personal computer, they are generally called cyber offence. Such as pornography, spreading rumors through social media, sharing someone's personal bad pictures through social media and online financial fraud, etc [1].

Cyber Crime exists on cyberspace. The word 'cyberspace' comes from Greek "kybernetes", that means governor, pilot, or rudder. Cyberspace is the global domain of electromagnetics accessed through electronic technology and exploited through the modulation of electromagnetic energy to achieve a wide rooted in range of communication and control system capabilities. Jones (1997) called cyberspace as a new public space. There are some cyber threats in the cyberspace, such as cyber espionage, cyber warfare, cybercrime, and cyber terrorism [2].

Cybercrime is a crime which involves the use of digital technologies in committing of offence, directed to computing and communication technologies. The modern techniques that are proliferating towards the use of internet activity results in creating exploitation, vulnerability making a suitable way for transferring confidential data to commit an offence through illegal activity [3].

It is defined as any criminal activity, which takes place on or over the medium of computers or internet or other technology recognized by the Information Technology Act. Not only the criminals are causing enormous losses to the society and the government but are also able to conceal their identity largely. There are number of illegal activities, which are committed over the internet by technically skilled criminals. Taking a wider interpretation, it can be said that, Cybercrime includes any illegal activity where computer or internet is either a tool or target or both.

According to Britannica dictionary, Cybercrime is also called Computer crime, the use of a computer as an instrument to further illegal ends, like committing fraud, trafficking in child pornography and intellectual property, stealing identities, or violating privacy. Cybercrime, especially through the Internet, has grown in importance as the computer has become central to commerce, entertainment and government [4].

Cybercrime is any criminal activity carried out in, on, or via the internet with the intention of defrauding, cheating, or causing a

network device, such as a computer, phone, or other device, to malfunction. The threat of cyber-crime and the capacity to respond to it will vary dramatically across nations. The expansion of computer connectivity increases risks to data privacy, setting new modes of criminal opportunity [5].

Cybercrime is generally described as a general term that refers to all criminal activities done using the means of computers, the internet, cyber space and the worldwide web. In other words, it is a crime in which a computer and its connected is the target of the crime being used as a tool to commit an offenes [6]. According to Hale (2002), in the current online era of cyber threats, a huge number of cyber threats and its impact along with understanding is difficult to restrict at the initial stage of the cyber-attacks [7]. The Muslim youth are more impressionable and seem to be naturally curious in everything they do around them in the society. The Muslim youths use the internet for research, amusement, and fun, which increases their risk of becoming victims of cybercrime. Cybercrime is one of the most common types of crimes in the recent generation.

2. Related Literature

The nature of this article requires an understanding of Cybercrime and Muslim lives from their main sources. Certain scholarly works have given an overview of the above. It is against this background that the article has set the context of academic work. In this regard a number of books and scholarly works which are on Cybercrime and Muslim lives are considered.

Smith, Grabosky and Urbas (2004) indicated that it is often complicated in getting a unique and consistent definition of cybercrime. This has resulted in a multiplicity of terms such as computer crime, computer-related crime, digital crime, information technology crime, internet crime, and virtual crime. Also, (Plot, 2010) look at cybercrime in the same dimension as Smith et, al., he proposed that there are several types of cybercrimes some of which include; cyber terrorism, fraud-identity theft, drug trafficking deals, malware, cyberstalking, spamming, logic bombs, and password sniffing. The use of a computer to accomplish illegal aims, such as scams, the trafficking of child pornography and intellectual property, identity theft, and privacy violations, is known as cybercrime, also referred to as computer crime. The use of a computer to accomplish illegal aims, such as scams, the trafficking of child pornography and intellectual property, identity theft, and privacy violations, is known as cybercrime, and some scholars also referred to it as computer crime.

But Maat (2004), argues and proposed a simple definition for cybercrime which encompasses all illegal activities where the computer, computer systems, information network or data is the target of the crime and those known illegal activities or crimes that are actively committed through or with the aid of computer, computer systems, information network or data. Cybercrime, according to Maat, is any criminal conduct where a computer or computer systems serve as the central mechanism that facilitates the activity.

Alkaabi, (2010) articulated that, traditionally, the term cybercrime referred to crimes over networks, especially the internet but the term has increasingly become a general term or replacement for computer. Accordingly, text messaging (SMS) and other methods and techniques can be used in cybercrime to gain access to a person's information through the usage of a network. But it is now broadly referred to as computer crime.

Christopher, U. et al., was of the view that, Cybercrime is a crime which involves the use of digital technologies in commission of offense, directed to computing and communication technologies. They further posit that the modern techniques that are proliferating towards the use of internet activity result in creating exploitation, vulnerability making a suitable way for transferring confidential data to commit an offense through illegal activity. This is a significant aspect in terms of cybercrime, and it will aid in the work explaining some of its impacts. This is a significant aspect in terms of cybercrime.

Thomas and Loader (2000), conceptualized cybercrime as those computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks.

3. Methodology

In the words of Guest et al., (2012) methodology is the general principle behind research. He further elaborates that methodology underpins the values and assumptions that form the rationale for the research. This article is basically qualitative. The data centered on both Primary and Secondary sources. Primary data formed the novel data that was collected from the field of study. The natural data was gathered through observations and participation in activities like conversing with youths in their various ghettos and sitting with them in internet cafés. The data was also sourced by interviewing native speakers from the community. The data was recorded, as well as jotting down the major points, and then used for the analysis. The research was also prepared based on secondary data, which was collected from different sources like books, journals, newspapers, and the Internet. The collected information has been analysed to draw suggestions from the study and make the study informative to the concerned readers. This technique of the critical review was demonstrated by cybercrimes and religious life of the Muslim youths.

The Target population consists of Thirty-Five (35) people. Five (5) non-Muslims and Thirty Muslims (30). The reason of the five non-Muslims was that; they were part of the youths in the interview grounds. These people are noted for their knowledge in the concept. When internet connectivity is available, they may do their daily business in their various houses instead of gathering mostly at internet cafés. The interviewer attended to them one after the other for them to respond to the questionnaire. This provided accurate data for the analysis in the study.

4. Results and Discussions

4.1. Islam and Crime

Islam teaches that justice is important both for the victim of a crime and the person accused of committing it. It must be proven that a person committed a crime before a punishment is set. which condemn (say it's wrong) the use of torture:

'Verily Allah will torture those who torture people in this world [8]

The Shariah has a very high level of proof for the most serious crimes and punishments. If proof is not as specified, then the crime must be considered a lesser crime. The major myth is that judges in Islamic nations have fixed punishments for all crimes. The judge under Shariah is not bound by precedents, rules, or prior decisions as in the common law.

Hadd crimes is the most serious crimes in the Shariah law, such as, murder, apostasy, making war upon Allah and His messengers, theft, adultery, defamation, false accusation of adultery or fornication, robbery and consumption of intoxicants. These are considered crimes against Allah.

Tazir crimes are acts which are punished because the offender disobeys Allah's law and word. Tazir crimes are crimes against society.

Qesas crime is one of retaliation. If you commit a Qesas crime, the victim has a right to seek retribution and retaliation. The concept of retribution was found in the first statutory "Code of Hammurabi" and in the law of Moses in the form of "an eye for an eye." Muslims add to that saying "but it is better to forgive." Contemporary common law today still is filled with the assumptions of retribution.

Many states have fixed punishment for drug, violence and the use of particular weapons. Qesas crime is simple retribution: if one commits a crime he knows what the punishment will be. Diya has its roots in Islamic law and dates to the time of the Prophet Mohammad (S.A.W) when there were many local families, tribes and clans. The Prophet was able to convince several tribes to take a monetary payment in retribution for damage to the clan or tribe. Diya is paid by the offender to the victim if he is alive. If the victim is dead, the money is paid to the victim's family or to the victim's clan or tribe.

The assumption is that victims will be compensated for their loss. Under English common law, the victim or family must sue the offender in a civil tort action for damages. Qesas law combines the process of criminal and civil hearings into one, just as the "civil law" is applied in many nations on Earth. Qesas crimes are compensated as restitution under common law and civil law. The Qesas crimes require compensation for each crime committed.

4.2. The Quran, Sunnah and Cybercrime

There is not clear picture of cybercrime in the Holy Quran and Sunnah of the Holy Prophet Muhammad (S.A.W), but there are related verses in condemning the activity and nature of the act of cybercrime. According to Islamic teachings, there are rules for chatting in public spaces. The following chapters in the Holy Quran address the issue of media;

There is no good in most of their conversations. Unless there is a person in it who orders alms, invites the righteous, or reconciles people who are in conflict [9].

O believers! Do not consume one another's wealth through unlawful means; instead, do business with mutual consent [10].

Male or female, whoever is guilty of theft, cut off their hand (that was used in theft) of either of them as a punishment for their crime. This is exemplary punishment ordained by Allah [11].

Allah commands you to give back the trusts to their rightful owners [12].

Prophet Mohammad (S.A.W) said:
'The signs of a hypocrite are three: Whenever he speaks, he tells a lie. Whenever he promises, he always breaks his promise. If you trust him, he proves to be dishonest. If you keep something as a trust with him, he will not return it' [13].

The Prophet Muhammad (S.A.W) used to communicate and convey his message effectively with wisdom. He taught his followers to speak nicely and softly.

The Prophet had been reported as;
'He who believes in Allah and the Last Day should either utter good words or better keep silence' [14].

A dishonest act is equivalent to fraud. Dishonesty is one of the worst forms of fraud. A dishonest person is always prone to defraud others whenever and wherever possible. Among the dishonest act or fraudulent activities are embezzlement, misappropriation, misapplication, destruction, removal, or concealment of property, alteration or falsification of paper or electronic documents, including the inappropriate destruction of paper or electronic documents, false claims and/or misrepresentation of facts, theft of an asset, trade secrets or intellectual property, inappropriate use of computer systems including hacking and software piracy, bribery, kickbacks, or rebates, conflict of interest or commitment.

Islamic law, being a complete legal system, seeks to repair the evils and enjoin the order in society in all aspects, including those dealing with protecting goods and security. Government can set up computer crime laws based on Islam which addresses the individual before the crime is committed and therefore is more of prevention than a cure.

4.3. Prevention of Cybercrimes in the Holy Quran

Islam is described as "a complete code of life" and it includes ethical conduct, belief, and worship. The corpus of Islamic teachings and laws is called Shariah, which provides the ethical foundation of conduct for either the individual or community.

Islamic teachings are the light for everyone and should be followed in every aspect of human life. As a Muslim we should act according to Islamic teaching, thoughts and believes in any condition and circumstances.

In this era of Modern Technology, IT has been used in Islamic Education as well as with Western Education. Students should be given education about cybercrimes and its impact on the lives of an individual as well as on the society.

Nowadays we are passing the modern era that depends on information technology and it is completely involved in our life. The web and networks has provided a suitable international background for people to store and send information, work, socialize, communicate, learn, buy, and sell etc, that has also opened a door for criminals to access un authentically to other person's data and information. Islam recommends that all sources of information should be in written form to save them for others or time when required.

Islam respects every one's information and privacy and does not allow anyone to spy about other's information or documents, cheat, and control others properties in any form.
In this regard Islamic teachings and punishments are very strict and clear for a person who interrupts or steals other properties like information, security, documents, and privacy.
Holy Quran:

"*Whoever does a wrong will be recompensed for it, and he will not find besides Allah a protector or a helper" [15].*

Information and documentations are viewed in Islam as very significant and valuable assets to gain knowledge and to achieve a successful Islamic society. Islam is very concerned with an effective communication. It reveals that only when a communication is free from any obstacles, the information will be safely conveyed and understood and thus directed to the truth.
Holy Quran:

"*O you: who believe! Fear Allah and speak a word right" [16].*

In order to respect the privacy of each Muslim society or community Allah Says in Quran:
"*O you: who believe! Avoid much suspicion; indeed some suspicion is sin. And spy not, neither backbite one another" [17].*

Holy Quran:
"A*nd do not consume one another's wealth unjustly or send it [in bribery] to the rulers in order that [they might aid] you [to] consume a portion of the wealth of the people in sin, while you know [it is unlawul]" [18].*

This verse provided the general meaning of fraud where Allah has prohibited Muslims to consume other's wealth unjustly. Therefore, any activities that lead to such action are considered as fraud. Islam forbids all types of fraud and all actions of deceiving, whether the fraud in buying and selling or in any other matter between people. All Muslim are urged to be honest and truthful in all situations in everything they do.

4.4. Access to Internet

The issue of having access to internet was asked to the respondents. Majority of the respondents has access to internet in their various homes. They acquired them because of the availability of social media. They used them to transact businesses actually known to them. Only few respondents do not have access to internet in their homes. Adam Allassan, a Sakawa was of the view that he has data for all the networks, which he acquire constantly every day in his phones [19].

4.5. Purpose of using Internet

The question on the purpose of using internet was an interesting one to the respondents as most of them involve in the same act of using the internet. The respondents of the same act were actually using the internet to transact sakawa and not for academic purpose. Only few of the respondents used the internet for academic purpose. The Muslim youths acquired a lot from the use of the internet. Therefore, it is necessary for them to acquire a lot of data in a day for that purpose. Afa Yushawu, an Arabic instructor, indicated that, the Muslim youths used the internet a lot because they gain from the use of it [20].

4.6. Own Social Media Account

When the researcher asked whether one own a social media account, majority of the respondents indicated 'yes' and only few did not have an account. Those who has an account indicate that, it is necessary to have an account before you embark on the work of sakawa. But those who do not have an account actually did not know anything on cybercrime. Mallam Yahaya, an Arabic scholar, indicated that those who has access to internet and used it for a purpose needs to have an internet accounts. He added that, he has nothing to do with using internet for selfish gains like sakawa, instead use it for research works [21].

5. Meaning of Cybercrime

On the question, what is cybercrime? The common answers were, it's a computer crime, hacking, negative use of social sites, misuse of an internet or technology, illegal use of a computer, not different from other crimes, crime by networking, criminal activities through computer via the internet. Some gave different answers as severe offence, uncontrollable, unethical, dangerous, cyber bullying, harassment, fraud, fake Facebook Id, invading privacy, technology attack, security lapse of the system designed, to put information at risk, crime which effect human culture of state, use any data without permission, search and misuse other's profile, target and spread computer viruses to other machines. Only few respondents identified or define cybercrime correctly while other did not reply because they don't know the cybercrime's definition and other respondents answered wrongly.

6. Types of Cybercrime among Muslim Youth

Muslims are always dominant in a Muslim community. Mostly

Christians are the second largest in the area follow by the followers of the traditional beliefs. Today most Muslims also adhered to the traditional principles. There are various cybercrimes found within the Muslim youths. These are found spreading very fast in search areas. The following were identified during the research considered to be the common types in a Muslim dominated area.

Pornography is common among the Muslim youths. The availability of the complex mobile phones is the cause of the rampant act among them. In the cafes, it is common the youth opens to internet, seeing or finding nude images of men and women. This slowly poison the mind by showing these images to children. Especially the young girls are tempted to take nude pictures and upload them on the internet. In an expectation that they get a lot of money.

Stalking someone on the Internet, harassing them by sending constant e-mails, entering chat rooms and making bad suggestions, etc. are common among the youths. Statistics show that, the youth are more likely to harass women through stalking.

Another type that is common in such areas are Stealing original information and disseminating false information so that the real information is not revealed. Many times 'saved' parents are subject to specific work, research and of course, intellectual property is stolen. Many times copyright, trademark, computer service code etc. are also stolen through the internet by the criminals of the cybercrime world. This mode sometimes called cybersquatting.

Illegal oppression and defamation on the net is common in the areas. Someone spread fake news on the internet about the Konkomba tribe preparing to attack Dagbamba. This information causes a lot of fear and panic in the area. Another defamation has spread across of the youth taking kidneys for monies from anyone of any age. This terrible information has been circulating on the internet day after day. Some self-interested people have done illegal oppression on people's minds.

Financial Fraud, credit card number withdrawals, bank fraud or online purchases all fall under this type of crime.

7. Reasons of Cybercrime

The respondents in answering the reasons why is the Cybercrime common among the Muslim youths, the first important reason for cybercrime is the proliferation of information, technology, and computers among the youth, which attracts cyber criminals. Majority of the respondents agreed that the influx of these items are the main reasons of cybercrime. Adam Alhassan, Café attendant, obviously confirmed that the mode of the youth having access to computers, mobile phones, and access to data of browsing is the main reasons of cybercrime [22].

Respondents are of the view that, cyber offenders are able to acquire critical competencies and skills in cyber and information technology to be more profitable in their field of work, which is increasing their work speed and spreading crime in the society. The existing law of Ghana, specifically the study area, against cybercrime is very complicated due to which cybercriminals have been able to get out of various loopholes of this law and from this possibility and opportunity, cybercrime has become more dynamic.

The research indicates that, nowadays the field of traditional crime is decreasing and law enforcement agencies are very vocal in enforcing the law, so cyber criminals have chosen cyber world as a dead possibility due to lack of this opportunity and spread their criminal activities there. Nowadays traditional crimes are some crimes or some acts that have been going on for a long time that cannot be changed suddenly. An important aspect in the cyber world is that, it is very easy to change, due to cyber criminals, have chosen an important factor in this world where from time to time they can change the nature of crime and is an important factor in the spread of cybercrime.

8. Causes of Cybercrime

The research outline that, since cybercrime is multi-directorial phenomena of modern society, it has so many causes considering the victimology and criminology. Most of the respondents pointed out that, both traditional crime and the computer crime occurred with help of latest technology against individual, organization, society and state. Cybercriminal does not commit crime only for financial gain, there are some other issues such as political, ideological, common conflict of business and personal issues. The respondents outline some major causes of cybercrime in the following areas.

Lack of Security Awareness: Due to the rapid coverage of internet facilities and social media usage, huge numbers of users have been included in cyber space daily. But they have no proper education and training on it or they have not enough awareness on its security measures. They just come and interact with other users blindly over computer or smart phone. Criminal people target them and breach sensitive information by gaining their account information as they do not use secured and strong password to their account or they use unauthorized software or content in their personal computer.

System error or weakness: Cheater or scammer or hacker finds out a system's error or weakness. After find out if they manipulate it for gaining unauthorized access. Development in IT sector is increased in very rapidly. So that various system and software is developed in short time. So errors or bugs remain in the system, due to the business plan they come in the market with that bugs. Then opponent hire hackers for finding it and for counter business policy.

Absence of relying Law frame work: Cyber technology and facilities have been growing day by day, at same time the criminal develops latest tools for their criminal activity but the state authority they do not have same effort in the race. Updating new legal frame work government needs enough time and financial capacity. So they may late to process new legal frame work. In that chance criminal are occurring crime in cyber space alarmingly.

Ignoring social and religious value: A Society or community is established based on some social and religious believe. For a peaceful and discipline society every member of that society need to follow their social and religious value. While some people have gone out of that value they are making exception. Every Exception has some affects and effects. Ignoring religious values, being a desperate toward life a cyber-user may interact in such way that is harmful for whole society.

Money gambling tendency: Modern people are reckless, they want have money anyhow and they want to be rich in a short time. So they try to find out shortcut ways

Social problem: There are so many problems in the society because of political and financial issues. Huge numbers of educated young generations are unemployment. So they always are trying for income source. Criminal people find out them and train up them and engage them in cybercrime.

Global Challenges or predominance: Modern age is waiting for third world war. Super power country always tries to show their power and predominance and try to control less developed country with technical advancement so trained up a group of cyber security specialist for their controlling. Common conflict: Modern people are revengeful and unrest in nature. Conflict in personal life or business, they try to do harm the opponent. So they try to find out a way for harming. As Cyber technology gives so many chances for targeting someone. That's why enraged people try to revenge upon the counterpart people.

9. Impact of Cybercrime

When a question was asked that, what impacts are being tabulated in the society because of hacking or any cybercrime activity? Their common answers were negative impacts were being tabulated such as, it affected self-confidence, destroying our youth, culture and society because of misuse of a personal information and blackmailing and trust is being eliminated in the society because of evil activity.

The different answers to it were that it had both positive and negative impact. Through positive hacking lots of crime can be stopped by anti-hackers, stressful environment, youth destroy their education while using computer in wrong activities through spreading and using personal information, feeling unsafe, torture, depression, less self-confidence, non-trust issues, people are scared of making social websites, dangerous impacts because of losing data and misusing pictures by Photoshop, society becomes more destructive because of misuse of a data, death rate is being high because of blackmailing, people facing a lot of troubles and taking tension, bring low confidence, hesitation or person cannot be able to face public, demoralization of personal lives, cyber criminals take full advantages of the anonymity, secrecy, and the interconnectedness provided by the internet. The impacts are harsh able, stress, violence, money stealing, personal life disruptions, abuse of young generation because of blackmailing, kidnapping etc. Only few respondents answered and majority respondents did not answer to this question.

10. Conclusion

The Study found that based on the perceptions of the Muslim Youth's cybercrime is prevalent and very common. A good number of Muslim Youths are into its practices. Many of the respondents were knowledgeable in cybercrime. Majority of them were able to identify modes and operations of cybercrime and their source of knowledge were indicated as friends, internet, radio and television. Therefore, education in any form whether formal or non-formal can be regarded as a good source of knowledge.

The study revealed that most of who engaged in cybercrime are Muslim Youths. The study revealed that respondents identified peer pressure, vengeance or payback, the quest for quick riches, poor parenting, fame, easy to practice and low chance of being caught, poverty, Internet literacy as the major inspiring causes for involvement in cybercrime. It appears from the study that Muslim Youths engagement in cybercrime had negative effects on the youth.

Therefore, Muslim youth's involvement in cybercrime led to their loss of faith. It came out of the study that getting arrested by police, going to jail, decrease ability to concentrate, poor academic performance, absenteeism and school dropout were some of the effects connected with cybercrime.

Criminals also try to hack face book accounts to misuse and blackmailing that causes stress and violence in society. In order to spread awareness about cybercrimes and their punishments, this study was done that shed light on information technology, cybercrime and criminal, their methods and protection from it by government policies and Quran and Sunnah.

It well defines the impact of cybercrime on the users of face book and their experiences about it. The results disclose that the victims of cybercrimes face a lot of stress and lost their confidence. The study also confirms that majority of people care about the religious values and they are not involved in these types of illegal activities. These crimes are also like other crimes. Those are not permissible by the governments and in Islam [23,24].

11. Recommendations

Cybercrime for the past years is considered as a worldwide phenomenon affecting almost individuals and nations and most countries consider it fight as a major priority. In view of this the following recommendations could be a great influence in the fight against cybercrime to either prevent or bring it down to a barest minimum among the youth especially the Muslim youth.

- Governments and Islam both formed some laws for prevention from these crimes. These laws are needed to be implemented immediately to get rid of cybercrimes and teach a lesson to cyber criminals.
- The study recommends that the schools 'curriculum must include courses on cybercrime to manage and educate students on the effect of cybercrimes on their studies.

- National Cyber Security Awareness Program (NCSAP) should endeavour to sponsor media (internet, radio and television) to strengthen and intensify education through awareness creation in order to have cybercrime free society. This can educate the public on the act, effects and other consequences of cybercrime to every citizen found anywhere in the community, school, mosques, churches and homes.
- The school authority should collaborate with parents to counsel and educate students on the effects on their engagement in cybercrime on their academic performance. The school can establish guidance and counselling unit in the school to give counselling to culprits within the school in various forms and also teach them morals.
- Considering the diverse nature of the cause of cybercrime it requires a collective approach between appropriate Ghanaian authorities and the citizenry in order to help fight this menace.
- The justice system must come out with policies to deal with all matters relating to cybercrimes by establishment of cybercrime courts in the country to prosecute cybercriminals and parents who do not take good care of their children by allowing them engage is such crime.
- They should also encourage more people to take up courses on cyber law and cybersecurity in a form of scholarship especially lawyers and judges within the justice system.
- Cybercrime is a worldwide canker which needs collaboration to deal with. Therefore, it needs intelligence and other best practices from countries that are able to chalk success in the fight against this crime such as United States of America, France, and Britain. Some of these cybercriminals acquire computer technologies from these countries to perpetuate such crimes. Therefore, cooperating with them can motivate them to effectively assist infighting this crime by blocking the sources they acquire those sophisticated computer software and technologies.
- The Ghana Police Service is not well resource in terms of training and tools to fight cybercrime in the country. This is why cybercrime is easy to practice with low chance of being caught. This therefore calls for improve training programmes with more concentration on ICT skills development. This will be equipped them with the knowledge to deal with different categories of cybercrime.

References

1. Effa-Ababio, K. (2005). The nature and dynamics of culture and its social, moral and religious dimensions. *Journal of Science and Technology (Ghana), 25*(2), 91-102.
2. Asadullah, A., Yerima, B., & Aliyu, Y. (2014). The ethics of information and communication technology: an Islamic overview. *International Journal of Information and Communication Technology Research, 4*(2).
3. Maghaireh, A. (2008). Shariah Law and Cyber-Sectarian Conflict: How can Islamic criminal law respond to cyber crime?. *International Journal of Cyber Criminology, 2*(2).
4. Baskerville, R. (1991). Risk analysis: an interpretive feasibility tool in justifying information systems security. *European Journal of Information Systems, 1*(2), 121-130.
5. Shamhuna, A. A. (2023). Cybercrime on the Socio-religious Lives of Muslim Youths. *Available at SSRN 4566797*.
6. Dashora, K., & Patel,P.P.(2025). Cyber crime in the society: Problems and preventions. *Journal of Alternative Perspectives in the social sciences, 2025, 3*(1), 240-259.
7. Shamhuna, A. A. (2023). Cybercrime on the Socio-religious Lives of Muslim Youths. *Available at SSRN 4566797*.
8. Furnell, S. M., & Warren, M. J. (1999). Computer hacking and cyber terrorism: The real threats in the new millennium?. *Computers & Security, 18*(1), 28-34.
9. Hassan, A. B., Lass, F. D., & Makinde, J. (2025). Cybercrime in Nigeria: Causes, effects and the way out. *ARPN Journal of Science and Technology, 2025,2*(7), 626-631.
10. Kandpal, V., & Singh, R. K. (2013). Latest face of cybercrime and its prevention in India. *International Journal of Basic and Applied Sciences, 2*(4), 150-156.
11. Khan, N. K. (2013). Cyber laws encompassing the Security of E-Quran in Saudi Arabia. *American Journal of Engineering Research, 2*(10), 253-257.
12. Leidner, D. E., & Kayworth, T. (2006). A review of culture in information systems research: Toward a theory of information technology culture conflict. *MIS quarterly*, 357-399.
13. Nathan, S. (2006). The Muslim Resurgence in Ghana since 1950.
14. Oumarou,M.(2025).Brainstorming advanced fee fraud:'Faymania'–the Camerounian experience. *Current trends in advance fee fraud in West Africa, EFCC, Nigeria, 2025*, 33-34.
15. Okpewho, I. (1992). *African Oral Literature*. Bloomington adn Indianapolis: Indiana University Press.
16. Plot, J. (2025). Top five computer crime and how to protect yourself from them. *Publication of Justin plot*.
17. Usmani, S. A. A., & Akmal, Z. (2018). Social Media and Its Impact on Secularism in Society. *The Islamic Culture" As-Saqafat-ul Islamia*.
18. Pazzack, A. P. (2013). Dagbani: An introductory course for beginners. *Koforidua: Pedaddo Ventures*.
19. Roger, B. (2004). *Dagbani-English Dictionary*. Tamale: Tamale Institute of Cross-Cultural Studies.
20. Rashid, M. A. (2017). Linguistic Relativity Among The Dagbamba. *International Journal of Innovative Research and Advanced studies (IJIRAS), 4*(11), 200-205.
21. Salifu Abdul Seidu's (2025) "Islam in Dagbon", Long Essay, both submitted to the Department for the study of Religions, University of Ghana
22. Loader, B. D., & Thomas, D.(Eds.).(2025). *Cybercrime: Law enforcement, security and surveillance in the information age*. Routledge.
23. Tayob, A., Ludwig, F., & Adogame, A. (2025). John Spencer Trimingham ,(2025) on Islam in Africa: integrative or isolationist?. *European Traditions in the Study of Religion in Africa, 2025*, 237.
24. Zulhuda, S. (2010, December). Information security in the Islamic perspective: The principles and practices. I*n Proceeding of the 3rd International Conference on Information and Communication Technology for the Moslem World (ICT4M) 2010* (pp. H-33). IEEE.

Oral Interviews

Adam Allassan, a Sakawa boy interviewed on the 6th of May 2023
Afa Yushawu, an Arabic instructor, interviewed on the 3rd March, 2023.
Alhassan Muhammed Dawuni (Chief of Tamale), interviewed on 21st January, 2017.
Mallam Yahaya, an Arabic scholar, interviewed on the 19th of March, 2023.
Mohammed Salman (Sakawa) interviewed on the 5th of May 2023