E-Journal of Humanities, Arts and Social Sciences (EHASS)
ISSN – Online 2720-7722 | Print 2821-8949
Volume 5 Issue 14 November 2024 pp 2597 – 2612
Available online at: https://noyam.org/journals/ehass/
DOI: https://doi.org/10.38159/ehass.202451411

Understanding Cybercrime in Developing Economies: Insights from Agona Swedru, Ghana

Charles Obeng[1], Paul Kwasi Kumah [1], Hubert Bimpeh Asiedu[1] & Felix Awuah Obeng Senior [1]
[1] Kwame Nkrumah University of Science and Technology, Kumasi-Ghana.

ABSTRACT
The purpose of this study was to explore the prevalence and primary causes of cybercrime in Agona Swedru. Using a quantitative research survey and a simple random sampling technique, 397 individuals were surveyed. The study's data were analyzed using both frequencies, cross tabulation and linear regression. The findings highlight that a significant proportion of the population engages in cybercrime, with online romance scams and financial fraud being the common forms of cybercrime being practiced. Unemployment, financial constraints, and poverty were identified as primary causes, pushing individuals towards cybercrime as a means to achieve financial stability. Based on the findings, it is recommended that enhancing employment opportunities through vocational training and job creation programs can alleviate the strain caused by unemployment. Also, establishing financial aid programs and counseling services can help individuals manage financial pressures. Implementing these recommendations will create a more stable and supportive environment, reducing the factors that drive individuals toward cybercrime. By identifying socioeconomic factors, such as unemployment and poverty, as key drivers of cybercrime, this study enhances understanding of the motivations behind cybercrime in Agona Swedru and similar contexts.

Correspondence
Charles Obeng
Email:
obengcharles436@gmail.com

Publication History
Received: 13th September, 2024
Accepted: 7th November, 2024
Published online: 28th November, 2024

Keywords: *Cybercrime, Unemployment, Financial Constraint, Poverty*

INTRODUCTION
In 2011, the UN reported that over 2.3 billion people, more than one-third of the global population, had internet access.[1] More than 60 percent of all internet users resided in developing countries, and 45 percent of these users were under 25 years old. By 2017, mobile broadband subscriptions were projected to reach nearly 70 percent of the world's population. By 2020, the number of networked devices (the 'internet of things') was expected to outnumber people by six to one, fundamentally altering understanding of the internet. In this hyperconnected future, it will be difficult to imagine a 'computer crime' or perhaps any crime that does not involve electronic evidence linked to internet protocol (IP) connectivity.[2] Despite the significant strides made in embracing digital transformation, countries around the globe are being threatened by cyber-attacks.[3] Cybercrime as defined by Anderson and colleagues encompasses traditional,

[1] United Nations Office on Drugs and Crime, " Comprehensive Study on Cybercrime," 2013, https://www.unodc.org/documents/organizedcrime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf
[2] United Nations Office on Drugs and Crime, " Comprehensive Study on Cybercrime."
[3] INTERPOL, " African Cyberthreat Assessment Report Cyberthreat Trends," 2023.

transitional, and novel offenses unique to the Internet.[4] Cybercrime has emerged as a pervasive and complex threat in the increasingly digitized world, transcending geographical boundaries and impacting individuals, businesses and nations alike.[5]

According to the UNODC reports cybercrime incidents have increased by approximately 30% annually over the past five years. In 2023, the Anti-Phishing Working Group (APWG) reported the third-highest quarterly total of phishing attacks ever recorded, with 1,286,208 incidents.[6] Additionally, Distributed Denial-of-Service (DDoS) attacks increased by 67% year-on-year and 24% quarter-on-quarter in the third quarter of 2022. The online industries experienced the most significant application-layer attacks, showing a 131% increase quarter-on-quarter and a 300% rise year-on-year in the number of attacks.[7] Recent statistics indicate that data breaches are a major concern, with 6.41 million data records leaked globally in the first quarter of 2023.[8] Furthermore, over 50% of medium and large UK businesses reported experiencing a cybersecurity breach or attack between April 2022 and April 2023.[9] Comparatively, North America and Europe report the highest number of incidents, primarily due to their advanced digital infrastructure and higher internet penetration rates. However, emerging economies in Asia, Africa, and Latin America are also experiencing a sharp rise in cybercrime activities as they continue to digitize.[10]

The issue of cybercrime has become a major concern in developing countries particularly in Africa in recent years. In 2017 alone Africa incurred a total of $3.5 billion in losses due to cybercrime.[11] For example, Nigeria is noted as a nation of 419 scammers (internet fraudsters).[12] Upon closer examination, it becomes evident that, compared to other African nations, Nigeria bears the highest financial burden from cybercrime, despite having the largest number of certified professionals. Ajala has argued that Nigeria's annual loss to cybercrime is approximately N127 billion, equivalent to 0.8 percent of the country's GDP. Meanwhile, the Financial Derivatives Company [FDC] reports that Nigeria's estimated annual financial losses related to cybercrime were N250 billion ($649 million) in 2017 and increased to N288 billion ($800 million) in 2018.[13] Cybercrime poses a threat to national security as it exposes individuals to violence, cyber espionage, cyberstalking, and manipulation. While certain young individuals have outrightly condemned the action, others have embraced it as a coping mechanism for unemployed, frustrated, and socioeconomically deprived Nigerian youth.[14]

This issue of cybercrimes is inevitable in their friendly sister country, Ghana. Similarly, the Ghana Police Service in its concerted efforts to mitigate the occurrence of cyber fraud, as disclosed by the Cybercrime Unit's reports, revealed that cyber fraud accounts for a significant 45% of all cybercrime cases in Ghana.[15] In support of this, Dr. Herbert Gustav Yankson, who serves as the Head of the Cybercrime Unit within the Criminal Investigation Department of the Ghana Police Service, has stated that the year 2020 witnessed a total financial loss of $19.8 million USD incurred by victims due to the actions of cybercriminals in the country.[16] Additionally, Dr. Yankson highlighted a 39% surge in cybercrime

[4] Ross Anderson et al., "Measuring the Cost of Cybercrime," *The Economics of Information Security and Privacy*, 2013,265–300.
[5] Shuai Chen et al., "Exploring the Global Geography of Cybercrime and Its Driving Forces," *Humanities and Social Sciences Communications* 10, no. 1 (2023): 1–10.
[6] Vishalkumar Ravindrakumar Gajjar and Hamed Taherdoost, "Cybercrime on a Global Scale: Trends, Policies, and Cybersecurity Strategies," in *2024 5th International Conference on Mobile Computing and Sustainable Informatics (ICMCSI)* (IEEE, 2024), 668–76.
[7] Cook S., " DDoS Statistics, Facts and Trends for 2018-2019tics-Facts/," Comparitech.com., 2018, https://www.comparitech.com/blog/information-security/ddosstatis.
[8] A. Petrosyan, " Data Breaches Worldwide," Statista, 2023, https://www.statista.com/topics/11610/databreaches-worldwide/.
[9] Fieldfisher, " Data Breach Agony - How to Limit the Likelihood of Eyewatering Fines," 2023, https://www.fieldfisher.com/en/insights/data-breach-agony-how-tolimit-the-likelihood-of-eye-watering-fine.
[10] Petrosyan, " Data Breaches Worldwide"; Gajjar and Taherdoost, "Cybercrime on a Global Scale: Trends, Policies, and Cybersecurity Strategies."
[11] Landry Signe and Kevin Signe, "Global Cybercrimes and Weak Cybersecurity Threaten Businesses in Africa," 2018, https://www.brookings.edu/blog/africa-infocus/2018/05/30/global-cybercrimes-and-weak-.
[12] Vaibhav Garg and L Jean Camp, "Why Cybercrime?," *Acm Sigcas Computers and Society* 45, no. 2 (2015): 20–28.
[13] Tope Shola Akinyetun, "Poverty, Cybercrime and National Security in Nigeria," *Journal of Contemporary Sociological Issues* 1, no. 2 (2021): 86–109.
[14] Sogo Angel Olofinbiyi, "Exploring Youth Awareness of Cybercrime and Factors Engendering Its Proliferation in Nigeria," *African Renaissance* 18, no. 4 (2021): 319.
[15] Abdul-Salam Shaibu, "Cybercrime: The Ghanaian Perspective," 2023.
[16] L. Tenyah-Ayettey, "Cyber Fraudsters Stole $19.8m in 2020," Daily Guide Network, February 2021, https://dailyguidenetwork.com/cyber-fraudsters-stole-19-8m-in-2020.

compared to the preceding year. Cyber fraud has emerged as the contemporary equivalent of traditional confidence tricksters, who once engaged people in person to manipulate them into relinquishing money or valuables, commonly known as '419.[17] In Ghana, various types of cybercrime activities abound, including online gold fraud, where individuals promote counterfeit gold through online advertisement. Given Ghana's prominence in gold mining, victims often fall prey to these deceptive schemes.[18] Additionally, there is the occurrence of online estate scams, wherein criminals pose as real estate agents offering assistance to Ghanaians living abroad who wish to construct a home in Ghana and relocate upon their retirement.[19] However, this phenomenon never occurs in isolation and is always influenced by contributing factors.

A study by ENISA (European Union Agency for Cybersecurity) highlights that human error and lack of awareness are major contributing factors to successful cyber-attacks.[20] To support this, a study by Baylon and Antwi-Boasiako proved that a prominent cause of cybercrime in Ghana is the lack of cybersecurity infrastructure and awareness. That is, many individuals and organizations in the country have limited knowledge about cybersecurity best practices, making them vulnerable to cyberattacks.[21] Additionally, Ennin and Mensah revealed that high levels of unemployment and poverty create a breeding ground for individuals seeking quick financial gains through illicit means, including cyber fraud and scams.[22] Furthermore, other studies in Ghana have noted that the rapid expansion of technology and internet access also fuels cybercrime in Ghana.[23] Given the ongoing relevance of these contributing factors, the impact of cybercrime on individuals and society at large cannot be overstated.[24]

Research by Grabosky illustrates the impact of cybercrime on trust in digital platforms, emphasizing that cybercrime erodes confidence in online interactions.[25] Furthermore, the economic implications of cyber threats on businesses and national security were highlighted. In Ghana, a study by Ghann and Owiredu documented a significant number of participants who mentioned a decline in customer trust as a consequence of cybercrime.[26] This erosion of confidence has resulted in the unfortunate loss of lives among customers and has contributed to a shortfall in the bank's revenue targets. As such several interventions have been put in place by regions and individual countries to reduce cybercrime.

Sustainable Development Goal (SDG) 16 aims to promote peaceful and inclusive societies, provide access to justice for all, and build effective, accountable institutions at all levels. This goal emphasizes the need to reduce violence, combat corruption, and ensure that governments are open and responsive to their citizens.[27] In relation to cybercrime, SDG 16 seeks to enhance the rule of law by addressing the growing threat of digital offenses, which undermine trust in institutions and jeopardize public safety. Effective measures against cybercrime are essential to achieving the broader objectives of peace, justice, and strong institutions envisioned by SDG 16.[28] In relation to this and in order to mitigate the issue of cybercrime in Ghana stakeholders such as government, NGOs and financial institutions have instituted various strategies and policies.[29] For instance, the Ghanaian government implemented the

[17] Shaibu, "Cybercrime: The Ghanaian Perspective."
[18] Edward Akuako, "The Sakawa Boys: A Critique of Policing of Cybercrime in Ghana.," 2022.
[19] Jason Warner, "Understanding Cyber-Crime in Ghana: A View from Below," *International Journal of Cyber Criminology* 5,no.1 (2011).
[20] Dimitra Markopoulou, Vagelis Papakonstantinou, and Paul de Hert, "The New EU Cybersecurity Framework: The NIS Directive, ENISA's Role and the General Data Protection Regulation," *Computer Law & Security Review* 35, no. 6 (November 2019): 105336, https://doi.org/10.1016/j.clsr.2019.06.007.
[21] Caroline Baylon and Albert Antwi-Boasiako, "Increasing Internet Connectivity While Combatting Cybercrime: Ghana as a Case Study," 2016.
[22] Daniel Ennin and Ronald Osei Mensah, "Cybercrime in Ghana and the Reaction of the Law," *JL Pol'y & Globalization* 84 (2019): 36.
[23] Ebenezer Acquah, " Critical Investigation of the Causes of Economic and Cyber Fraud among the Youth in Africa: A Case of Ghana," *The International Journal of Business & Management* 6, no. 6 (2018).
[24] Ennin and Mensah, "Cybercrime in Ghana and the Reaction of the Law."
[25] Peter N Grabosky, "Virtual Criminality: Old Wine in New Bottles?," in *Cyberspace Crime* (Routledge, 2017), 75–81.
[26] Patricia Ghann and Joseph Owiredu, "The Effect of Cybercrime on Financial Institutions: A Case Study of Mumuadu Rural Bank, Osino in the Fanteakwa District-Eastern Region, Ghana," 2022.
[27] United Nations, "SDG 16: Promote Peaceful and Inclusive Societies for Sustainable Development, Provide Access to Justice for All and Build Effective, Accountable and Inclusive Institutions at All Levels," Department of Economic and Social Affairs, 2023, https://sdgs.un.org/goals/goal16.
[28] Kempe Ronald Hope Sr, "Peace, Justice and Inclusive Institutions: Overcoming Challenges to the Implementation of Sustainable Development Goal 16," *Global Change, Peace & Security* 32, no. 1 (2020): 57–77.
[29] Ministry of Communications, " Ghana National Cyber Security Policy & Strategy. Republic of Ghana," July 2015, https://www.academia.edu/37141183/NATIONAL_CYBER_SECURITY_POLICY_AN D_STRATEGY_REPUBLIC_OF_GHANA?pdf;

National Cyber Security Policy and Strategy (NCSP&S) as an institutional framework.[30] In 2015, the Ministry of Communications adopted the NCSP&S to combat cyber fraud and formulate measures for the implementation and enforcement of cybercrime laws.[31] Additionally, in December 2020, the government further reinforced its commitment to cybersecurity by enacting the Cybersecurity Ac. This legislative move aimed to enhance Ghana's cybersecurity capabilities. The Cybersecurity Act, established in 2020, focuses on creating a cybersecurity authority, safeguarding the nation's critical information infrastructure, regulating cybersecurity activities, and ensuring the protection of children on the internet. This strategic initiative contributes to the overall development of Ghana's cybersecurity ecosystem.[32]

Despite the numerous global and individual national efforts to mitigate the issue of cybercrime, cybercrime continues to persist particularly in developing countries like Ghana, especially in Agona Swedru, where the act of cybercrime has become a primary pursuit and goal for many young individuals, underscoring the need to understand the key factors contributing to its prevalence. For instance, a study by Akuako revealed that approximately 70% of young individuals in Agona Swedru are engaged in cybercrime (Sakawa) or express a desire to engage in such activities.[33] Therefore, this study aims to fill this gap by exploring the prevalence and primary causes of cybercrime in Agona Swedru. Specifically, the study intends to examine the prevalence of cybercrime and the primary causes of cybercrime. The subsequent sections of this study focus on the theoretical framework, literature review, methodology, presentation of findings, and policy implications/ recommendations respectively.

It is as a result of this aim that the researchers seek to answer the following research questions.

1. What cybercrime activities are most prevalent in Agona Swedru?
2. What are the primary causes of cybercrime in Agona Swerdru?

THEORETICAL FRAMEWORK

In this study, Robert K. Merton's Strain Theory was utilized, chosen for its capacity to offer a conceptual framework that elucidates how certain social factors, can potentially compel individuals to resort to cybercrime as a coping mechanism.The Strain Theory, proposed in 1938, suggests that crime is a result of the strain or disconnect between culturally prescribed goals and the legitimate means available to achieve those goals.[34] Merton argued that societies promote certain culturally approved goals, such as wealth and success, and individuals are expected to strive toward these goals. However, not everyone has equal access to the approved means (legitimate avenues) for achieving these goals.[35] This theory therefore provides a comprehensive understanding of the prevalence and causes of cybercrime.

Many citizens in developing countries face significant socio-economic challenges, including high levels of unemployment, poverty, financial constraints and limited access to education and resources.[36] These conditions create a strain between societal expectations for success and the actual means available to achieve these goals. The Strain Theory suggests that when people are unable to achieve success through conventional methods, such as education and stable employment, they may resort to alternative means, including criminal activities, to attain their goals.[37] Cybercrime in Ghana has become a prevalent issue, often attributed to the country's rapid adoption of digital technologies amid economic hardship. For many Ghanaians, especially the youth, the allure of cybercrime stems from the perception that it offers a quicker, more accessible route to financial success compared to the traditional pathways that seem blocked by systemic barriers. This aligns with Merton's concept of "innovation," where individuals accept societal goals but use illegitimate means to achieve them. In this case, cybercriminals

Ghann and Owiredu, "The Effect of Cybercrime on Financial Institutions: A Case Study of Mumuadu Rural Bank, Osino in the Fanteakwa District-Eastern Region, Ghana."

[30] Ministry of Communications, " Ghana National Cyber Security Policy & Strategy. Republic of Ghana."

[31] Ministry of Communication and Digitalisation, "Cybersecurity Act Passed to Promote & Regulate Cybersecurity Activities," 2020, https://www.moc.gov.gh/cybersecurity-act-passed promote-regulate-cybersecurity-activities.

[32] Ministry of Communication and Digitalisation, "Cybersecurity Act Passed to Promote & Regulate Cybersecurity Activities."

[33] Akuako, "The Sakawa Boys: A Critique of Policing of Cybercrime in Ghana."

[34] R. K. Merton, " Social Structure and Anomie," in *Gangs*, ed. Jacqueline Schneider (London: Routledge, 2017), 3–13.

[35] Merton, " Social Structure and Anomie."

[36] Ghann and Owiredu, "The Effect of Cybercrime on Financial Institutions: A Case Study of Mumuadu Rural Bank, Osino in the Fanteakwa District-Eastern Region, Ghana."

[37] Carter Hay and Katherine Ray, "General Strain Theory and Cybercrime," *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, 2020, 583–600.

recognize the value placed on wealth and success but innovate through illegal digital activities to attain these ends.[38]

LITERATURE REVIEW

Cybercrime in Ghana

The prevalence of cybercrime issues in Ghana has grown over the past years.[39] For instance, the Cybercrime Unit of the Ghana Police Service reported the following numbers of cybercrime cases from 2016 to 2022; 116 cases in 2016, 412 cases in 2017, 558 cases in 2018, 600 cases in 2019, 1097 cases in 2020, 1147 cases in 2021 and 1077 cases in 2022. This data has prompted the Police Service to enhance educational and awareness efforts among the public to mitigate the menace. The figures reveal a consistent upward trend in the number of cases from 2016 to 2021, with a slight decrease observed in 2022.[40] He attributed this rise to the impact of the COVID-19 pandemic, noting that a greater number of individuals engaged in online business transactions as opposed to in-person dealings.[41] Additionally, Adu and Adjei, posit that a significant number of organizations, specifically 50 (77%), recognized the heightened risk of falling prey to cybercrime due to the escalating frequency of cyber-attacks.[42] Cybercrime activities in Ghana come in many forms such as Cyberfraud, Intrusion, gold fraud, online estate scam, malware and online romance scam.

Cyber fraud in Ghana is the act of utilizing the internet to unlawfully obtain money, food, services, etc., from individuals through deceptive means, commonly referred to as '419'. Instances of fraud within this realm of cybercrime encompass email fraud, criminal activities conducted via online banking, and fraudulent schemes on various regional payment and mobile banking platforms.[43] This is estimated to make up approximately 45% of all reported cybercrime cases in Ghana, according to information from the Cybercrime Unit of the Police Service.[44] For instance, in 2019 Bank of Ghana's the year under review period; there was a 34.48% reduction in cyber fraud cases, declining from 174 instances in 2018 to 114 cases in 2019. Despite this decrease, cyber fraud still represented the largest attempted fraud amounting to GH₵ 50.54 million, with an actual loss of GH₵14.31 million.[45] Again, in the 2022 Bank of Ghana's report detailing an overview of various attempted and successful fraudulent activities reported by Ghana's Banking Institutions, Specialized Deposit-Taken Institutions (SDIs) and Payment Service Providers (PSPs); the report provided that 12,166 cases of mobile money frauds were recorded in the year 2022 as against 12,350 cases recorded in 2021 which shows a quite reduction.[46]

Also, unauthorized access occurs when criminals, without permission, target the digital and networking systems of their victims with the intent to steal valuable network resources, collect user information, pilfer data and documents, disrupt data-related activities, or inflict damage on or corrupt systems.[47] Examples of such intrusions include hacking and data breaches. For instance, the hacking incidents involving Ghanaian government websites in early 2015 exemplify attacks directed at government technology infrastructure. In 2016, the Electoral Commission of Ghana experienced a website hack during the transmission of election results. In April 2017, media houses' websites were subjected to Distributed Denial of Service (DDoS) attacks. In 2022, the Electricity Company of Ghana (ECG) fell victim to a weeks-long hacking of its prepaid vending system, leading to customers being unable to purchase prepaid services.[48] Unauthorized access encompasses various forms, including website defacement and unauthorized modification.[49]

---

[38] R. K. Merton, *Social Theory and Social Structure* (Simon and Schuster, 1968); Merton, " Social Structure and Anomie."
[39] Shaibu, "Cybercrime: The Ghanaian Perspective."
[40] Shaibu, "Cybercrime: The Ghanaian Perspective."
[41] Tenyah-Ayettey, "Cyber Fraudsters Stole $19.8m in 2020."
[42] Kofi Koranteng Adu and Emmanuel Adjei, "The Phenomenon of Data Loss and Cyber Security Issues in Ghana," *Foresight* 20, no. 2 (2018): 150–61.
[43] Bank of Ghana, " The 2019 Fraud Review Report," 2019, bog.gov.gh.
[44] Shaibu, "Cybercrime: The Ghanaian Perspective."
[45] Bank of Ghana, " The 2019 Fraud Review Report."
[46] Kwafo Eric, " Modern Ghana News," 2022, https://www.modernghana.com/news/1238369/12166-cases-of-mobile-money-fraud-recorded-in.html.
[47] Shaibu, "Cybercrime: The Ghanaian Perspective."
[48] Ghana Business News, " ECG Systems Hacked with Ransomware ," 2022, ECG systems hacked with ransomware – Sources %7C GhHeadlines Total News Total Information.
[49] Shaibu, "Cybercrime: The Ghanaian Perspective."

Again, gold fraud takes place when individuals involved in gold scams share counterfeit images and videos advertising or showcasing gold purportedly for sale. In certain instances, these representations later prove to be gold-plated tungsten.[50] By utilizing fabricated images and videos, individuals involved in gold scams manipulate their targets into providing substantial sums of money for the purported transportation of gold from mining sites or specific locations to the receiver for a supposed sale transaction. After receiving payment for the alleged transportation, the scammers employ various excuses to justify their inability to deliver the gold to the location. These excuses serve as a pretext to request additional funds, ostensibly to facilitate the gold's delivery, ultimately revealing the entire operation to be a deceitful scheme. In tandem with this strategy, scammers also dispatch small amounts of gold (in grams or a kilo) intentionally, aiming to build trust and confidence with their victims while demonstrating their claimed ability to provide larger quantities. Once the victim's trust is established, the scammers demand substantial sums of money before vanishing, leaving the victims disillusioned.[51] For example, in September 2020, a businessman lost One Million Dollars ($1m) to a gold scam in Ghana.[52] Such a form of scam is most often successful because Ghana is believed to be endowed with gold and most victims believe the fraudsters to be gold dealers so far as they are from Ghana. For example, a report revealed that Ghana became the premier gold-producing country in Africa and sixth in the world with a production of 138.7 tons in 2020.[53]

Additionally, in recent years, Ghana has unfortunately witnessed a surge in real estate scams and fraud. These deceitful activities entail misleading individuals into investing in properties that either do not exist or do not justify the amount paid, presenting a substantial risk to both potential buyers and sellers.[54] Similar to online gold fraud, this scheme involves perpetrators reaching out to victims, primarily Ghanaians residing abroad, offering assistance in constructing houses in Ghana. They pose as real estate agents, targeting Ghanaians living abroad who may be interested in building a home in Ghana for their retirement.[55] Exploiting this pretext, the perpetrators deceive victims into sending money from overseas for the purported construction projects. Additionally, the perpetrators recognize that establishing a fraudulent online real estate business presents an attractive investment opportunity for individuals residing abroad. Consequently, they persuade potential victims to invest in properties like lands and hotels. Frequently, the fraudsters provide victims with counterfeit documents supposedly issued by the Ghanaian government, including land documents from the land commission and business certificates from the Registrar General Department.[56] In some instances, they create duplicate websites designed to mimic legitimate ones or redirect individuals to authentic websites.[57] An illustration of such a scenario surfaced in an online publication, *The Herald*, in November 2023. The incident involved a dispute over a three-bedroom apartment situated in Accra, owned by Imperial Homes Limited, a real estate developer. This disagreement resulted in allegations of fraud, prompting Ernest Danso to file a complaint at the Airport Police Station. Danso claimed that he had paid $270,000 as the apartment's purchase price. However, after residing in the property for three years, his ownership was challenged, leading to his forceful eviction and abandonment of his belongings. Court proceedings unveiled that the same property had been sold to another individual for $1 million USD. The central issue revolved around certain officials at Imperial Homes Limited forging their superior's signature to sell the house without providing proper notice to the company.[58]

Furthermore**,** malicious software, commonly known as malware, is specifically created with the intent to engage in criminal activities or inflict damage upon computer systems. Attackers employ various

[50] Akuako, "The Sakawa Boys: A Critique of Policing of Cybercrime in Ghana."
[51] Akuako, "The Sakawa Boys: A Critique of Policing of Cybercrime in Ghana."
[52] Ghana Web. (2020), Gold scams in Ghana - Mitigating the risk of fraud (ghanaweb.com)
[53] Ghana Web, "Gold Scams in Ghana - Mitigating the Risk of Fraud," 2020, Gold Scams in Ghana - Mitigating the risk of fraud (ghanaweb.com).
[54] Ghana Web, "Gold Scams in Ghana - Mitigating the Risk of Fraud."
[55] Akuako, "The Sakawa Boys: A Critique of Policing of Cybercrime in Ghana."
[56] Warner, "Understanding Cyber-Crime in Ghana: A View from Below."; Akuako, "The Sakawa Boys: A Critique of Policing of Cybercrime in Ghana."
[57] Frank A Duah and Asirifi Michael Kwabena, "The Impact of Cyber Crime on the Development of Electronic Business in Ghana," *European Journal of Business and Social Sciences* 4, no. 1 (2015): 22–34.
[58] The Herald, " Imperial Homes Caught up in US$270,000 Fraud Case," 2023, https://theheraldghana.com/imperial-homes-limited-property-caught-up-in-us270000-fraud-case/.

forms of malware such as worms, ransomware, adware, trojans and spyware to achieve their nefarious objectives.[59] Cyber attackers deploy viruses, worms, Trojan horses, adware, and spyware across the digital realm to target individuals, businesses, and governmental websites, aiming to gather crucial information. In the study conducted by Danquah the findings and subsequent analysis revealed that, in the realm of malware baselining, viruses emerge as the predominant form of malware infections.[60] Despite this prevalence, the associated consequences appear to be relatively minor. Notably, third-party mobile devices, laptops, and computers emerge as the primary targets for infection within the Ghanaian microfinance sector. Additionally, the study identifies advanced persistent threats as a formidable challenge that has yet to be effectively addressed.[61] Moreover, according to a study conducted by Adu and Adjei in 2018, 25% of organizations in Ghana encounter malware infections on an occasional basis.[62]

Moreover, in the realm of cyberspace, online dating and romance scams manifest through the 'man-woman format' or 'gender role' as well as 'gender-swapping'.[63] This entails 'male switching' scammers posing as females on the internet by creating deceptive profiles featuring sensual images of women, often models, to entice men (particularly those from Western countries) into relationships with the ultimate aim of financial exploitation. Achieving success in these scams involves the adept use of skills and tactics in the art of deception to establish seemingly authentic connections.[64] Additionally, online romance scam could in the idea of takes place when a perpetrator (Male or female) assumes a false online identity to establish trust and affection with a victim. Exploiting the illusion of a romantic or intimate connection, the scammer manipulates and steals from the victim, often by coercing them into sharing nude photos. Subsequently, these photos may be used to extort money, with threats of publication if the victim fails to comply.[65] With regards to the males, young men pose as females to entice other men, particularly sugar daddies, a practice commonly referred to as 'KKD'.[66] In a recent study by Abubakari, the findings suggest that the sociocultural backgrounds of female scammers, when coupled with the inherent opportunities provided by the internet, significantly contribute to the emergence of women in online romance frauds in the Tamale region of Ghana.[67]

According to Business World Publishing, Ghana's Cyber Security Authority estimates that victims have incurred losses of 49.5 million Ghanaian cedi ($4.5 million) due to identity theft schemes since the beginning of the year. In the same report, it was asserted that, in every slum in Accra, eight out of every ten youths are engaged in online romance scams. In an interview, a perpetrator named Starflex adopts the persona of Joan, a 23-year-old master's student from Turkey, while conversing with an American realtor he befriended on the online dating site Zoosk.[68] The fictitious Joan's boyfriend, unaware of the deception, believes her parents succumbed to COVID-19 and have been persuaded to cover her $5,000 tuition to prevent her deportation. Starflex (posing as Joan) discloses that the boyfriend sends $500 monthly for upkeep from the United States.[69]

From the literature, there is a consensus that cybercrime in Ghana has significantly increased over recent years, with the COVID-19 pandemic intensifying online activities and exposing individuals and organizations to heightened cyber threats. Scholars and reports agree that cyber fraud, such as romance scams, online estate scams, and gold fraud, is among the most prevalent forms, often involving elaborate

[59] Akuako, "The Sakawa Boys: A Critique of Policing of Cybercrime in Ghana."; Shaibu, "Cybercrime: The Ghanaian Perspective."
[60] Paul Asante Danquah, "MALWARE AND ANTI-MALWARE BASELINE: AN INDUCTIVE STUDY OF GHANAIAN MICROFINANCE COMPANIES.," *Information Technologist* 17, no. 1 (2020).
[61] Danquah, "MALWARE AND ANTI-MALWARE BASELINE: AN INDUCTIVE STUDY OF GHANAIAN MICROFINANCE COMPANIES."
[62] Adu and Adjei, "The Phenomenon of Data Loss and Cyber Security Issues in Ghana."
[63] Ann Cassiman, "Spiders on the World Wide Web: Cyber Trickery and Gender Fraud among Youth in an Accra *Zongo*," *Social Anthropology* 27, no. 3 (August 26, 2019): 486–500, https://doi.org/10.1111/1469-8676.12678; J. Burrell, *Invisible Users: Youth in the Internet Cafés of Urban Ghana* (The MIT Press, 2012).
[64] Abdul-Razak Kuyini Alhassan and Abukari Ridwan, "Identity Expression—the Case of 'Sakawa'Boys in Ghana," *Human Arenas* 6, no. 2 (2023): 242–63.
[65] Shaibu, "Cybercrime: The Ghanaian Perspective."
[66] Akuako, "The Sakawa Boys: A Critique of Policing of Cybercrime in Ghana."
[67] Yushawu Abubakari, "The Espouse of Women in the Online Romance Fraud World: Role of Sociocultural Experiences and Digital Technologies," *Deviant Behavior* 45, no. 5 (2024): 708–35.
[68] Business World Publishing, " Meet Ghana's Online Romance Scammers," 2023, https://www.bworldonline.com/world/2023/08/17/540206/meet-ghanas-online-romance-scammers/.
[69] Business World Publishing, " Meet Ghana's Online Romance Scammers."

deception tactics that exploit victims' trust and cultural expectations.[70] Disagreements are evident in the specific causes of the rise in cybercrime, with some attributing it to economic factors and technological accessibility, while others focus on sociocultural influences, particularly with regard to romance scams. Furthermore, studies reveal that unauthorized access, malware, and identity theft are growing concerns for Ghana's organizations, with implications for sectors such as banking and microfinance.[71] Overall, the literature concludes that cybercrime presents a formidable challenge in Ghana, urging intensified cybersecurity measures, public awareness initiatives, and strategic interventions to curb the impact of cyber threats on individuals and institutions.

METHODOLOGY

The primary data for this study was collected from young individuals in Agona Swedru. Agona Swedru is the capital of the Agona West Municipal Assembly with an overall population of close to 160,000 with 85,000 females and 75,000 males. The town is located in the northeast part of the central region, directly North of Winneba about 30km from the Accra – Cape Coast road.[72] The choice of this case is motivated by the prevalence of cybercrime activities in the community. As stated by Ninson, Agona Swedru is recognized as the central hub of cybercrime, particularly the practice known as "sakawa," in Ghana.[73] For example, research conducted by Akuako indicated that around 70% of young individuals in Agona Swedru are involved in cybercrime, specifically "Sakawa" or scamming, or aspire to participate in these illicit activities. Therefore, understanding the prevalence and the primary causes of cybercrime is crucial for devising effective strategies to combat cybercrime in Ghana, specifically in Agona Swedru.

A quantitative survey research design was adopted due to its systematic and organized approach to gathering and analyzing numerical data to validate hypotheses, investigate relationships, and draw statistical conclusions.[74] Quantitative research employs statistical methods for data analysis and interpretation.[75] To gather this data, a probability sampling design known as the simple random sample approach was utilized, ensuring that every young individual in Agona Swedru had an equal chance of being included in the research, thereby enhancing the representativeness and generalizability of the findings. The optimal sample size was determined using the Yamane formula, based on the total youth population in Agona Swedru (12,284), resulting in a sample of 397 young individuals. Structured questionnaires, featuring closed-ended questions on a five-point Likert scale (ranging from Strongly Agree to Strongly Disagree), were used as the primary data collection method.[76] Respondents were randomly selected and given the questionnaire at internet cafes, returning it upon completion.

Measures

Dependent variable: The dependent variable for the study is cybercrime. The prevalence of cybercrime was measured using a series of survey questions designed to capture various forms of cybercriminal activities in which participants might engage or might have fallen victim. These included unauthorized access to computers, online fraud, and participation in cyber-attacks. Respondents were asked to indicate the frequency of occurrence of such activities using a five-point Likert scale ranging from strongly agree to strongly disagree.

Independent Variable: The independent variable for the study is financial constraint. This was assessed by asking respondents about their access to financial resources, ability to obtain credit, and overall financial health. Questions included items like "How often do you find it difficult to meet your financial needs?" and "Have you ever been denied a loan due to lack of collateral?" Responses were recorded on a

[70] Akuako, "The Sakawa Boys: A Critique of Policing of Cybercrime in Ghana."
[71] Shaibu, "Cybercrime: The Ghanaian Perspective."
[72] Ghana Statistical Service, "The 2021 Population and Housing Census of Ghana General Report. Vol 3B," 2021, https://census2021.statsghana.gov.gh/gssmain/fileUpload/reportthemesub/2021 PHC General Report Vol 3B_Age and Sex Profile_181121b.pdf.
[73] Comfort Ninson, " Internet Fraud and Its Socio-Economic Implications for Peace and Development of Agona Swedru (Ghana)" (University of Cape Coast, 2017).
[74] Alan Bryman, *Social Research Methods* (Oxford university press, 2016).
[75] Bryman, *Social Research Methods*.
[76] Ghana Statistical Service, "The 2021 Population and Housing Census of Ghana General Report. Vol 3B."

five-point Likert scale ranging from "strongly agree" to "strongly disagree." Unemployment, poverty, broken homes and peer pressure were measured through an open-ended question that asked the respondent to provide the primary cause(s) of cybercrime, which was recoded into yes or no responses for the analysis. These measures aimed to capture both the prevalence of cybercrime and the contributing factors, providing a comprehensive understanding of the relationship between financial constraints, unemployment, poverty, broken home environments, peer pressure, and cybercrime among the youth in Agona Swedru.

Analytic Methods

The study utilized descriptive statistics, including crosstabs and frequencies, to analyze the prevalence of cybercrime. To determine the relationships among the dependent and independent variables, binary regression analysis was employed. The data was processed and analyzed using the Statistical Package for the Social Sciences (SPSS v22).

Ethical Considerations

The study took into account several ethical considerations to ensure the integrity and fairness of the research process. Prior to participating in the study, participants were provided with clear and comprehensive information about the research objectives, procedures, potential risks, and benefits. They were given the opportunity to ask questions and voluntarily consented to participate without any coercion or undue influence. Also, participants' identities and personal information were kept confidential and data were anonymized to ensure that individuals could not be identified from the findings. This safeguarded participants' privacy and protected sensitive information from unauthorized access. Furthermore, the study adhered to principles of non-maleficence and beneficence. Measures were taken to minimize any potential harm or distress to participants. The research team ensured that questions in the questionnaire were not intrusive or offensive and that participants were not exposed to undue psychological or emotional stress. Overall, by addressing these ethical considerations, the study maintained high standards of ethical conduct, prioritized the well-being and rights of participants, and upheld the credibility and trustworthiness of the research outcomes.

PRESENTATION OF FINDINGS

Prevalence of Cybercrime

Table 1 below provides a crosstabulation of respondents who have engaged in various types of cybercrime. From the survey, out of 397 respondents, 303 (76.4%) admitted to having engaged in cybercrime, while the remaining 93 (23.6%) indicated they had not. With regards to the kind or type of cybercrime practiced, online romance crime locally named “KKD” exhibits the highest prevalence, with 230 out of 303 respondents (75.9%) admitting to engaging in this type of cybercrime. This suggests that online romance scams are the most common form of cybercrime among the respondents, possibly due to the exploitation of emotional vulnerabilities and the potential for significant financial gain. Also, the second most common cybercrime is financial scams or frauds, with 148 respondents (48.8%) involved. Financial scams can include activities like phishing, online banking fraud, mobile money fraud and other deceptive practices aimed at stealing money or financial information. Additionally, 75 respondents (24.8%) have engaged in identity theft. This type of cybercrime involves stealing personal information to commit fraud or other crimes. With 32 respondents (10.6%) involved, online harassment or cyberbullying highlights the use of digital platforms to harass or bully individuals. Although less prevalent compared to financial scams and romance scams, its impact on victims can be severe.

Online estate scam, involving 23 respondents (7.6%), typically targets individuals looking to rent or buy property online, exploiting the anonymity and reach of the internet. Moreover, the least common type of cybercrime among the respondents is gold fraud, with 22 respondents (7.3%) involved. This usually involves the sale of fake or non-existent gold investments.

Table 1: Crosstabulation of Respondents Who Have Engaged in Cybercrime and the Type of Cybercrime Practiced

	Cybercrime	

			Financial scam or fraud	Identity theft	Gold fraud	Online estate scam	Online romance scam	Online harassment or cyber bullying	Total
Do you or have you engaged in cybercrime of any form	Yes		148 (48.8%)	75 (24.8%)	22 (7.3%)	23 (7.6%)	230 (75.9%)	32 (10.6%)	303
Total			148	75	22	23	230	32	303
Percentages and totals are based on respondents.									
a. Dichotomy group tabulated at value 1.									

Primary Causes of Cybercrime

Table 2 presents data on the primary causes of cybercrime as identified by survey respondents. From the survey, unemployment was identified as the leading cause of cybercrime, accounting for nearly one-third of 161 (29.0%) of the responses. This indicates that a lack of job opportunities may drive individuals to engage in illegal online activities as a means of income. Again, financial constraint was the second most cited cause, with over a fifth of 128 (23.1) of the respondents attributing their involvement in cybercrime to economic pressures. This highlights the role of financial desperation in motivating individuals to commit cybercrimes. Also, poverty, affecting 81(14.6%) of the respondents, underscores the broader socioeconomic factors that contribute to cybercrime. The overlap with financial constraints suggests that economic hardship, in general, is a significant driver. Furthermore, peer influence accounts for 97(17.5%) of responses, indicating that social circles and the pressure to conform to group behaviors play a crucial role in the decision to engage in cybercrime. Moreover, the impact of a broken home on cybercrime involvement is notable, with 88(15.9%) of respondents citing it as a cause. This suggests that family instability or dysfunction can push individuals towards criminal activities online.

Table 2: Primary Causes of Cybercrime

		Responses	
		N	**Percent**
Causes of cybercrime	Unemployment	161	29.0%
	Financial constraint	128	23.1%
	Poverty	81	14.6%
	Broken home	88	15.9%
	Peer-influence	97	17.5%
Total		**555**	**100.0%**

a. Dichotomy group tabulated at value 1

From Table 3 financial constraints emerged as the most significant predictor of cybercrime, with an unstandardized coefficient of 0.294 and a value of 0.000, indicating a strong and statistically significant positive relationship. This means that as financial constraints increase, the likelihood of engaging in cybercrime also increases. Unemployment also shows a significant positive relationship with cybercrime, with an unstandardized coefficient of 0.190 and a significant level of 0.013, indicating that higher unemployment rates are associated with higher cybercrime rates. Furthermore, poverty has a significant positive impact on cybercrime, with an unstandardized coefficient of 0.186 and a p-value of 0.037, suggesting that individuals in poverty are more likely to engage in cybercrime, possibly due to financial desperation and lack of legitimate means to improve their economic situation.

Table 3: Regression Results on Causes of Cybercrime

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	1.625	.410		3.960	.000
	Finconstraint	.294	.062	.232	4.777	.000
	Unemployment	.190	.076	.127	2.502	.013
	Poverty	.186	.089	.102	2.092	.037
	Broken home	.126	.087	.071	1.443	.150
	Peer-influence	.090	.085	.053	1.057	.291
a. *Dependent Variable: Cybercrime*						

DISCUSSION

The Prevalence of Cybercrime in Agona Swedru

The aim of the first objective of the study was to explore the prevalence of cybercrime and the study found that a significant proportion of the respondents have engaged in cybercrime, with over three-quarters admitting to such activities. This means that cybercrime is a prevalent issue among the surveyed population, highlighting the need for comprehensive understanding and targeted interventions. This resonates with Merton's Strain Theory, which posits that societal pressure and the strain caused by the inability to achieve culturally prescribed goals through legitimate means can lead individuals to resort to criminal behavior as a coping mechanism.[77] The high prevalence of cybercrime among respondents aligns with the idea that social inequality and financial constraints play a crucial role in driving such behaviors.[78]

Moreover, the findings show that online romance scams, locally known as "KKD," are the most common form of cybercrime, with the majority of respondents admitting to participating in these scams. This means that exploiting emotional vulnerabilities and leveraging the promise of romantic relationships is a particularly effective strategy for cybercriminals. This resonates with Merton's concept of innovation, where individuals accept societal goals but use illegitimate means to achieve them.[79] In this case, the societal goal is financial success, and the illegitimate means are engaging in online romance scams. Empirical studies support this finding, as evidenced by research indicating in the realm of cyberspace, online dating, and romance scams manifest through the 'man-woman format' or 'gender role' as well as 'gender-swapping'.[80] The study also found that financial scams or frauds are the second most common type of cybercrime among the respondents. This means that many individuals engage in activities such as phishing, online banking fraud, and mobile money fraud to steal money or financial information. This finding aligns with Merton's Strain Theory, as financial constraints and unemployment drive individuals to seek alternative, often illegal means to achieve financial stability.[81] Empirical studies corroborate this, highlighting the significant financial impact of cyber fraud in Ghana and the variety of fraudulent activities prevalent in the country.[82] Furthermore, the study revealed that identity theft is also widespread, highlighting the ease with which personal information can be stolen for fraudulent purposes, further supporting the theory and empirical findings of substantial financial losses in Ghana.[83] Online harassment or cyberbullying, although less prevalent, poses severe impacts on victims and reflects the aggressive behaviors stemming from frustration and strain. Additionally, less common cybercrimes like online estate scams and gold fraud indicate the use of deception in property and investment scams, aligning with the theoretical framework of seeking financial success through illegitimate means.[84]

[77] Merton, " Social Structure and Anomie."
[78] Ghann and Owiredu, "The Effect of Cybercrime on Financial Institutions: A Case Study of Mumuadu Rural Bank, Osino in the Fanteakwa District-Eastern Region, Ghana."
[79] Merton, " Social Structure and Anomie."
[80] Cassiman, "Spiders on the World Wide Web: Cyber Trickery and Gender Fraud among Youth in an Accra *Zongo*"; Burrell, *Invisible Users: Youth in the Internet Cafés of Urban Ghana*.
[81] Merton, " Social Structure and Anomie."
[82] Shaibu, "Cybercrime: The Ghanaian Perspective."
[83] Business World Publishing, " Meet Ghana's Online Romance Scammers."
[84] Merton, " Social Structure and Anomie."

The primary causes of cybercrime in Agona Swedru

The second objective of the study was to identify the primary causes of cybercrime. From the data collected unemployment was identified as the leading cause of cybercrime. To support this, the regression result also revealed a significant positive relationship between unemployment and cybercrime indicating that a lack of job opportunities may drive individuals to engage in illegal online activities as a means of income. This finding resonates with Merton's Strain Theory, which posits that when individuals are unable to achieve societal goals through legitimate means, they may resort to illegitimate methods.[85] In Ghana, significant socio-economic challenges such as high unemployment rates create a strain that compels many to seek alternative, often illegal, avenues for financial success.[86] Empirical studies have documented the rise in cybercrime cases in Ghana, supporting the notion that economic hardship is a significant driver of such activities.[87] Additionally, financial constraints were the second most cited cause, highlighting the role of financial desperation in motivating individuals to commit cybercrimes.

To support this regression result also revealed a significant positive relationship between financial constraint and cybercrime. This aligns with Merton's theory where financial pressures act as a strain, leading individuals to innovate through criminal activities to achieve financial stability.[88] The empirical data on the increasing number of cybercrime cases and the significant financial losses reported in Ghana further underscores the impact of financial constraints on the prevalence of cybercrime.[89] The study also found that poverty is a significant factor contributing to cybercrime. This underscores the broader socio-economic issues that drive individuals towards criminal activities. The overlap with financial constraints suggests that economic hardship, in general, is a significant driver. Merton's Strain Theory explains this phenomenon as the disconnect between societal expectations and the means available to achieve them, leading to strain and resultant deviant behavior.[90] In the context of Ghana, widespread poverty and limited access to resources exacerbate this strain, pushing individuals towards cybercrime as an alternative means to achieve economic goals.[91] Peer influence was also a notable factor, indicating that social circles and the pressure to conform to group behaviors play a crucial role in the decision to engage in cybercrime. This finding is consistent with the notion that individuals often turn to crime due to the influence of their immediate social environment, a concept supported by empirical studies that highlight the role of peer pressure in cybercriminal activities.[92] The empirical review shows that peer influence is a significant factor in the rising trend of cybercrime in Ghana, where social dynamics often encourage such behaviors.[93] Moreover, the impact of a broken home on cybercrime involvement suggests that family instability or dysfunction can push individuals toward criminal activities online. This finding is in line with Merton's theory, which acknowledges that social structures, including family, play a crucial role in shaping individual behavior.[94] Empirical studies have shown that family breakdowns contribute to a lack of social control and support, leading individuals to seek alternative, often illicit, means to cope with their circumstances.[95]

Discussion Summary

The study's findings highlight a significant prevalence of cybercrime, driven primarily by socio-economic factors such as unemployment, financial constraints, and poverty. These results align with Merton's Strain Theory, which suggests that the inability to achieve societal goals through legitimate means compels individuals to resort to criminal behavior, including online scams and fraud. Additionally, the influence

[85] Merton, " Social Structure and Anomie."
[86] Ghann and Owiredu, "The Effect of Cybercrime on Financial Institutions: A Case Study of Mumuadu Rural Bank, Osino in the Fanteakwa District-Eastern Region, Ghana."
[87] Shaibu, "Cybercrime: The Ghanaian Perspective"; K.A. Barfi, P. Nyagorme, and N. Yeboah, "The Internet Users and Cybercrime in Ghana: Evidence from Senior High School in Brong Ahafo Region," 2018, https://digitalcommons.unl.edu/libphilprac/1715/.
[88] Merton, " Social Structure and Anomie."
[89] Tenyah-Ayettey, "Cyber Fraudsters Stole $19.8m in 2020."
[90] Merton, *Social Theory and Social Structure*; Merton, " Social Structure and Anomie."
[91] Hay and Ray, "General Strain Theory and Cybercrime."
[92] Hay and Ray, "General Strain Theory and Cybercrime."
[93] Adu and Adjei, "The Phenomenon of Data Loss and Cyber Security Issues in Ghana."
[94] Merton, " Social Structure and Anomie."
[95] Shaibu, "Cybercrime: The Ghanaian Perspective."

of peers and family instability further exacerbates the situation, indicating the need for targeted interventions to address both the economic and social root causes of cybercrime in the region.

POLICY IMPLICATIONS/ RECOMMENDATIONS

To address the root causes of cybercrime, policymakers should devise their policies towards these recommendations. Firstly, enhancing employment opportunities through vocational training and job creation programs can alleviate the strain caused by unemployment. By conducting needs assessments and partnering with local businesses and educational institutions, relevant skills can be developed, leading to increased job opportunities. Secondly, establishing financial aid programs and counseling services can help individuals manage financial pressures. Microfinance initiatives and financial literacy programs will empower individuals to pursue lawful economic activities, reducing their reliance on illegal means. Lastly, strengthening social and family support systems through community-based support programs can mitigate the influence of negative peer pressure and family dysfunction. Establishing community centers, providing family counseling, and implementing mentorship and peer education programs will foster a supportive environment, encouraging positive behaviors. By addressing these key areas, the recommendations aim to create a more stable and supportive community, ultimately reducing the prevalence of cybercrime.

CONCLUSION

This study sought to explore the prevalence and underlying drivers of cybercrime in Ghana, specifically Agona Swedru. Through a quantitative descriptive analysis, the findings have indicated that factors like unemployment, poverty, and financial strain are not only prevalent but are critical catalysts for cybercrime. Ultimately, this study emphasizes that addressing cybercrime in the region requires not only enforcement but also comprehensive social and economic reform. By tackling the root causes of cybercrime, society can foster pathways for individuals to achieve their goals through legitimate means, reducing the appeal of criminal alternatives. These findings contribute to the broader discourse on crime prevention, urging stakeholders to prioritize both social and economic solutions in developing effective cybercrime policies.

BIBLIOGRAPHY

Abubakari, Yushawu. “The Espouse of Women in the Online Romance Fraud World: Role of Sociocultural Experiences and Digital Technologies.” *Deviant Behavior* 45, no. 5 (2024): 708–35.

Acquah, Ebenezer. “ Critical Investigation of the Causes of Economic and Cyber Fraud among the Youth in Africa: A Case of Ghana.” *The International Journal of Business & Management* 6, no. 6 (2018).

Adu, Kofi Koranteng, and Emmanuel Adjei. “The Phenomenon of Data Loss and Cyber Security Issues in Ghana.” *Foresight* 20, no. 2 (2018): 150–61.

Akinyetun, Tope Shola. “Poverty, Cybercrime and National Security in Nigeria.” *Journal of Contemporary Sociological Issues* 1, no. 2 (2021): 86–109.

Akuako, Edward. “The Sakawa Boys: A Critique of Policing of Cybercrime in Ghana.,” 2022.

Alhassan, Abdul-Razak Kuyini, and Abukari Ridwan. “Identity Expression—the Case of ‘Sakawa’Boys in Ghana.” *Human Arenas* 6, no. 2 (2023): 242–63.

Anderson, Ross, Chris Barton, Rainer Böhme, Richard Clayton, Michel J G Van Eeten, Michael Levi, Tyler Moore, and Stefan Savage. “Measuring the Cost of Cybercrime.” *The Economics of Information Security and Privacy*, 2013, 265–300.

Bank of Ghana. “ The 2019 Fraud Review Report,” 2019. bog.gov.gh.

Barfi, K.A., P. Nyagorme, and N. Yeboah. “The Internet Users and Cybercrime in Ghana: Evidence from Senior High School in Brong Ahafo Region,” 2018. https://digitalcommons.unl.edu/libphilprac/1715/.

Baylon, Caroline, and Albert Antwi-Boasiako. “Increasing Internet Connectivity While Combatting Cybercrime: Ghana as a Case Study,” 2016.

Bryman, Alan. *Social Research Methods*. Oxford university press, 2016.

Burrell, J. *Invisible Users: Youth in the Internet Cafés of Urban Ghana*. The MIT Press, 2012.

Business World Publishing. “ Meet Ghana’s Online Romance Scammers,” 2023. https://www.bworldonline.com/world/2023/08/17/540206/meet-ghanas-online-romance-

scammers/.
Cassiman, Ann. “Spiders on the World Wide Web: Cyber Trickery and Gender Fraud among Youth in an Accra *Zongo*.” *Social Anthropology* 27, no. 3 (August 26, 2019): 486–500. https://doi.org/10.1111/1469-8676.12678.
Chen, Shuai, Mengmeng Hao, Fangyu Ding, Dong Jiang, Jiping Dong, Shize Zhang, Qiquan Guo, and Chundong Gao. “Exploring the Global Geography of Cybercrime and Its Driving Forces.” *Humanities and Social Sciences Communications* 10, no. 1 (2023): 1–10.
Cook S. “ DDoS Statistics, Facts and Trends for 2018-2019tics-Facts/.” Comparitech.com., 2018. https://www.comparitech.com/blog/information-security/ddosstatis.
Danquah, Paul Asante. “Malware And Anti-Malware Baseline: An Inductive Study Of Ghanaian Microfinance Companies.” *Information Technologist* 17, no. 1 (2020).
Duah, Frank A, and Asirifi Michael Kwabena. “The Impact of Cyber Crime on the Development of Electronic Business in Ghana.” *European Journal of Business and Social Sciences* 4, no. 1 (2015): 22–34.
Ennin, Daniel, and Ronald Osei Mensah. “Cybercrime in Ghana and the Reaction of the Law.” *JL Pol’y & Globalization* 84 (2019): 36.
Fieldfisher. “ Data Breach Agony - How to Limit the Likelihood of Eyewatering Fines,” 2023. https://www.fieldfisher.com/en/insights/data-breach-agony-how-tolimit-the-likelihood-of-eye-watering-fine.
Gajjar, Vishalkumar Ravindrakumar, and Hamed Taherdoost. “Cybercrime on a Global Scale: Trends, Policies, and Cybersecurity Strategies.” In *2024 5th International Conference on Mobile Computing and Sustainable Informatics (ICMCSI)*, 668–76. IEEE, 2024.
Garg, Vaibhav, and L Jean Camp. “Why Cybercrime?” *Acm Sigcas Computers and Society* 45, no. 2 (2015): 20–28.
Ghana Business News. “ ECG Systems Hacked with Ransomware ,” 2022. ECG systems hacked with ransomware – Sources %7C GhHeadlines Total News Total Information.
Ghana Statistical Service. “The 2021 Population and Housing Census of Ghana General Report. Vol 3B,” 2021. https://census2021.statsghana.gov.gh/gssmain/fileUpload/reportthemesub/2021 PHC General Report Vol 3B_Age and Sex Profile_181121b.pdf.
Ghana Web. “Gold Scams in Ghana - Mitigating the Risk of Fraud,” 2020. Gold Scams in Ghana - Mitigating the risk of fraud (ghanaweb.com).
Ghann, Patricia, and Joseph Owiredu. “The Effect of Cybercrime on Financial Institutions: A Case Study of Mumuadu Rural Bank, Osino in the Fanteakwa District-Eastern Region, Ghana,” 2022.
Grabosky, Peter N. “Virtual Criminality: Old Wine in New Bottles?” In *Cyberspace Crime*, 75–81. Routledge, 2017.
Hay, Carter, and Katherine Ray. “General Strain Theory and Cybercrime.” *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, 2020, 583–600.
Hope Sr, Kempe Ronald. “Peace, Justice and Inclusive Institutions: Overcoming Challenges to the Implementation of Sustainable Development Goal 16.” *Global Change, Peace & Security* 32, no. 1 (2020): 57–77.
INTERPOL. “ African Cyberthreat Assessment Report Cyberthreat Trends,” 2023.
Kwafo Eric. “ Modern Ghana News,” 2022. https://www.modernghana.com/news/1238369/12166-cases-of-mobile-money-fraud-recorded-in.html.
Markopoulou, Dimitra, Vagelis Papakonstantinou, and Paul de Hert. “The New EU Cybersecurity Framework: The NIS Directive, ENISA’s Role and the General Data Protection Regulation.” *Computer Law & Security Review* 35, no. 6 (November 2019): 105336. https://doi.org/10.1016/j.clsr.2019.06.007.
Merton, R. K. “ Social Structure and Anomie.” In *Gangs*, edited by Jacqueline Schneider, 3–13. London: Routledge, 2017.
———. *Social Theory and Social Structure*. Simon and Schuster, 1968.
Ministry of Communication and Digitalisation. “Cybersecurity Act Passed to Promote & Regulate Cybersecurity Activities,” 2020. https://www.moc.gov.gh/cybersecurity-act-passed promote-regulate-cybersecurity-activities.

Ministry of Communications. " Ghana National Cyber Security Policy & Strategy. Republic of Ghana," July 2015. https://www.academia.edu/37141183/NATIONAL_CYBER_SECURITY_POLICY_AND_STRATEGY_REPUBLIC_OF_GHANA?pdf.

Ninson, Comfort. " Internet Fraud and Its Socio-Economic Implications for Peace and Development of Agona Swedru (Ghana)." University of Cape Coast, 2017.

Olofinbiyi, Sogo Angel. "Exploring Youth Awareness of Cybercrime and Factors Engendering Its Proliferation in Nigeria." *African Renaissance* 18, no. 4 (2021): 319.

Petrosyan, A. " Data Breaches Worldwide." Statista, 2023. https://www.statista.com/topics/11610/databreaches-worldwide/.

Shaibu, Abdul-Salam. "Cybercrime: The Ghanaian Perspective," 2023.

Signe, Landry, and Kevin Signe. "Global Cybercrimes and Weak Cybersecurity Threaten Businesses in Africa," 2018. https://www.brookings.edu/blog/africa-infocus/2018/05/30/global-cybercrimes-and-weak-.

Tenyah-Ayettey, L. "Cyber Fraudsters Stole $19.8m in 2020." Daily Guide Network, February 2021. https://dailyguidenetwork.com/cyber-fraudsters-stole-19-8m-in-2020.

The Herald. " Imperial Homes Caught up in US$270,000 Fraud Case," 2023. https://theheraldghana.com/imperial-homes-limited-property-caught-up-in-us270000-fraud-case/.

United Nations. "SDG 16: Promote Peaceful and Inclusive Societies for Sustainable Development, Provide Access to Justice for All and Build Effective, Accountable and Inclusive Institutions at All Levels." Department of Economic and Social Affairs, 2023. https://sdgs.un.org/goals/goal16.

United Nations Office on Drugs and Crime. " Comprehensive Study on Cybercrime," 2013. https://www.unodc.org/documents/organizedcrime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.

Warner, Jason. "Understanding Cyber-Crime in Ghana: A View from Below." *International Journal of Cyber Criminology* 5, no. 1 (2011).

ABOUT AUTHORS

Mr. Charles Obeng is currently a Teaching and Research Assistant in the Department of Sociology and Social Work at Kwame Nkrumah University of Science and Technology (KNUST), Kumasi, Ghana. He holds a Bachelor of Arts in Sociology (KNUST) with first-class honors. He is a multi-disciplinary trained researcher whose works extend into various areas of sociology and health. His research interests include education, publich health, criminology, business and politics. His current studies focus on examining the impact of health information technology on patients care quality and efficiency in public hospitals in Ghana, as well as enhancing students' interest and academic performance through innovative teaching methods such as discussion and multimedia.

Rev. Fr. Dr. Paul Kwasi Kumah is an ordained Priest of the Catholic Archdiocese of Kumasi, Lecturer in sociology with research interest in crime, education, and religion. He holds a PhD in Sociology from the KNUST, MPhil in Sociology from the KNUST, M.Ed. in Educational Administration from the University of Cape Coast, PGDE in Education from the University of Cape Coast, Bachelor of Arts in Sociology and the study of Religions from the University of Ghana, Legon, Bachelor of Sacred Theology from the Pontifical Urbaniana University in Rome. Rev.Fr. Dr. Kumah has Certificates in Criminology from the University of Queensland, Australia, Philosophy from the St. Paul's Major Seminary in Accra and Sacred Theology from the St. Peter's Major Seminary in Cape Coast, Ghana. Research interests include Sociology of Education, Criminology and criminal Justice and Religion.

Dr. Hubert received his B/A in Sociology and Study of Religion from the University of Ghana, Legon in 2004 and moved on to attain his MPhil in Sociology of Education at the University of Cape Coast, Ghana in 2011. He later had his PhD in Sociology at the University of Auckland, New Zealand in 2018. His other qualifications are Postgraduate Diploma in Education, University of Cape Coast (2004),and Postgraduate Diploma in Organizational Development, University of Cape Coast (2014). His research interest includes education, religion and criminology.

Mr. Felix Awuah Obeng Senior is an emerging Scholar who holds an Honours degree in Sociology from Kwame Nkrumah University of Science and Technology (KNUST), Ghana, where he is currently pursuing his MPhil in Sociology. His research focuses on three key areas: Crime and Deviance, Sociology of Food and Nutrition, examining cultural practices and food security; and Indigenous Knowledge and Practices. Through his involvement in multiple research projects, he contributes to both academic discourse and social development initiatives.