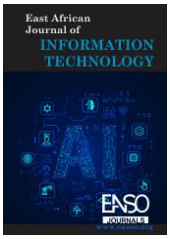
Article DOI: https://doi.org/10.37284/eajit.5.1.673



**East African Journal of Information Technology**
eajit.eanso.org
**Volume 5, Issue 1, 2022**
**Print ISSN: 2707-5346 | Online ISSN: 2707-5354**
Title DOI: https://doi.org/10.37284/2707-5354

EAST AFRICAN NATURE & SCIENCE ORGANIZATION

*Original Article*

# Internet fraud: The influence of Identity Flexibility and Dissociative Anonymity

*Paul Danquah*[1*], *John Amoako Kani*[1] & *Dzifa Bibi*[1]

[1] Heritage Christian College, P. O. Box AN 16798, Accra, Ghana.
* Correspondence ORCID: https://orcid.org/0000-0003-0528-5829; email: pdx017a@hcuc.edu.gh.

**Article DOI: https://doi.org/10.37284/eajit.5.1.673**

**Date Published:**

*19 May 2022*

**Keywords**:

*Internet Fraud, Identity Flexibility, Dissociative Anonymity*

## ABSTRACT

The purpose of this paper is to investigate the influence of identity flexibility and dissociative anonymity on internet fraud, focusing on the cyber deception and theft. Four victims, three culprits, and an experimental website were used to collect data for case study analysis. The researchers employed qualitative and quantitative data analysis for the study. Content analysis of interview transcriptions and results obtained from experimental website were used as the main data collection sources and tools. This study found that victims of internet fraud were defrauded by culprits who clearly practiced the application of identity flexibility and dissociative anonymity in their illegal endeavours. Despite the authenticity of registered crime related users on the experimented website, the true/actual identity of users could not be confirmed even though their credentials were technically validated before being saved. Findings shown in the study confirm the theoretical postulate that "identity flexibility, dissociative anonymity and lack of deterrence factor in the cyberspace provides the offenders the choice to commit cybercrime". The findings are also consistent with extant studies on the isolated studies that indicate anonymity as the trump card of most cyber criminals. Findings from culprits suggests that they make a conscious effort to satisfy all requirements but without genuine identification and credentials. Practical implications study provides some recommendations for fraud prevention on the internet. The major one is the need for practitioners and future researchers to emphasize on development of solutions that serve as a reliable check on authenticity of users as well as deterrent to all fraudulent users. This study is original, as it focuses on internet fraud that is highly pervasive as per previous research findings.

Article DOI: https://doi.org/10.37284/eajit.5.1.673

**APA CITATION**

Danquah, P., Kani, J. A., & Bibi, D. (2022). Internet fraud: The influence of Identity Flexibility and Dissociative Anonymity. *East African Journal of Information Technology*, *5*(1), 39-52. https://doi.org/10.37284/eajit.5.1.673

**CHICAGO CITATION**

Danquah, Paul, John Amoako Kani & Dzifa Bibi. 2022. "Internet fraud: The influence of Identity Flexibility and Dissociative Anonymity". *East African Journal of Information Technology* 5 (1), 39-52. https://doi.org/10.37284/eajit.5.1.673.

**HARVARD CITATION**

Danquah, P., Kani, J. A., & Bibi D. (2022) "Internet fraud: The influence of Identity Flexibility and Dissociative Anonymity", *East African Journal of Information Technology*, 5(1), pp. 39-52. doi: 10.37284/eajit.5.1.673.

**IEEE CITATION**

P. Danquah., J. A. Kani., & D. Bibi. "Internet fraud: The influence of Identity Flexibility and Dissociative Anonymity", *EAJIT*, vol. 5, no. 1, pp. 39-52, May. 2022.

**MLA CITATION**

Danquah, Paul, John Amoako Kani & Dzifa Bibi. "Internet fraud: The influence of Identity Flexibility and Dissociative Anonymity". *East African Journal of Education Studies*, Vol. 5, no. 1, May. 2022, pp. 39-52, doi:10.37284/eajit.5.1.673.

## INTRODUCTION

Internet fraud is a range of illegal and illicit actions that are committed in cyberspace, it is a type of cybercrime fraud or deception which makes use of the Internet. This could involve hiding of information or providing incorrect information for the purpose of tricking victims to obtain money, property, and inheritance (Brenner, 2009). It was explained that identity flexibility, dissociative anonymity, and lack of deterrence factor in the cyberspace provides the offenders the choice to commit cybercrime (Jaishankar, 2008). This has been reinforced via various research work such as that on cyber incivility, this is a form of nonconformity conduct, often experienced by users in this period of online media technology sophistication. Research efforts have been ongoing to understand cyber incivility in order to reduce and anticipate this dangerous behaviour in its various forms (Febriana & Fajrianthi, 2019).

Identity is defined as "the totality of one's self-construal, in which how one construes oneself in the present expresses the continuity between how one construes oneself as one was in the past and how one construes oneself as one aspires to be in the future"(Weinreich, 1986).

Identity flexibility is therefore defined as the ability of an individual to alter either partially or completely the self-construal and return to its original when needed. Dissociative Anonymity on the other hand describes situations where the acting person's identity is unknown and a distort perception detaches one from self or environment (Wallace, 1999).

Concerns have been expressed and research has looked closely at the subject from diverse perspectives, typical examples are namely; Barlett and Gentile (2014), Danquah (2015), and Danquah & Longe (2011). Research by Wada et al., (2012) and Febriana and Fajrianthi (2019) have also been done in line with anonymity.

The foundations of most of these articles were the Space Transition Theory (Jaishankar, 2008) which deductively attempted to theorize the varying human behaviour in the physical world as opposed to the cyber world. The further deduced model by Longe et al., (2012) from the theory as shown in figure 1 outlined specific factors as the influence of online behaviour. Figure 1 specifically outlines the various possible factors that could influence the commission of cybercrime as namely; valued status and position, identity anonymity with no deterrence factor, closed society, cyber world strangers, open society, and physical world associates. Emphasis in the context of this research is the dissociative anonymity with no deterrence factor component. The factors being assessed for the purpose of this research have not been specifically tested in any previous related research work hence the objective of this study. It is worth noting, however, that other scholars have shown via empirical tests that some aspects of the Space Transition Theory (STT) do not apply in certain contexts (Danquah & Longe, 2011). Evidently missing in most of this research work is

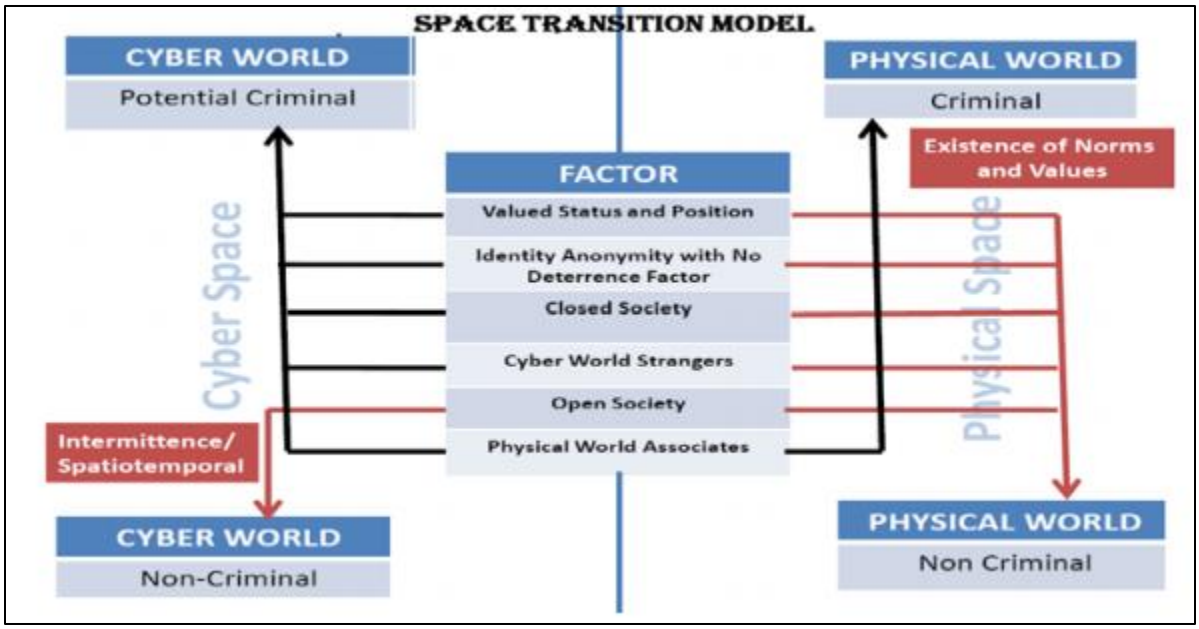
 

Article DOI: https://doi.org/10.37284/eajit.5.1.673

the absence of focusing on the combination of identity flexibility and dissociative anonymity's influence on commission of internet fraud.

The objective of this research work is therefore to assess the influence of identity flexibility and dissociative anonymity in the occurrence of internet fraud.

**Figure 1: Space Transition Model**




Source: (Longe, Danquah & Ebem, 2012)

It is hoped that this article can inspire researchers to investigate further the influence of Identity Flexibility, Dissociative Anonymity & Intermittent cyber ventures to encourage practitioners to develop policies and actions regarding online behaviour to reduce and anticipate the effects of internet fraud.

## LITERATURE REVIEW

It has been observed in other findings that while online, some people self-disclose or act out more frequently or intensely than they would in person. One research that explored numerous factors that interact with each other in creating online disinhibition effect looked at "dissociative anonymity, invisibility, a synchronicity, solipsistic introjection, dissociative imagination, and minimization of authority" (Suler, 2004). The findings from this research proved that personality variables also will influence the extent of this disinhibition.

In Barlett & Gentile (2014), the research on anonymity suggested that anonymity is related to positive attitudes toward cyberbullying and cyberbullying frequency, essentially anonymity was identified as one important risk factor for future cyberbullying behaviour.

An instructive method for internet fraud is the socially engineered cyber deception and theft (SECT), SECT is a form of cybercrime that involves a perpetrator using computer system to leverage on gained-trust from a victim and subsequently fraudulently exploiting the victim (Danquah et al., 2020).

Experiments carried out by Danquah and Longe (2011) and Danquah and Longe (2012) confirmed some postulates and disproved others for the space transition theory. The research outcome indicated some boundaries in the variety of cybercrimes are committed and practiced in Ghana. In Danquah et al. (2020), the crucial inference for the socially engineered cyber deception and theft are the

Article DOI: https://doi.org/10.37284/eajit.5.1.673

postulates which advise that identity flexibility, dissociative anonymity, lack of deterrence factor, and intermittent ventures of offenders in the cyberspace provides the offenders the choice to commit cybercrime and escape.

The effort of Longe et al. (2012), added to enhanced appreciation of cyber activities with a focus on tracking cyber fraudsters. This, possibly, served Danquah and Longe (2011) a premise to build upon the new knowledge gained to carry out an ethnographic study on cyber criminality in Ghana, whereas the follow-up study, Longe and Danquah (2012) specifically assessed socially engineered cyber deception and theft via an ethnographic study. An additional upshot Danquah and Longe (2013) did further work by investigating cyber deception and theft for which they investigated into, and beyond, E-Mail header in socially engineered cyber deception and theft. The outcome of this study showed that dissociative anonymity is a major contributing influence on cyber deception and theft. Numerous circumstances evaluated in the Longe et. al. (2012), Danquah and Longe (2011), and Danquah et al., (2013) expounded on the method used by the fraudsters to socially engineer cyber deception and theft.

Wada et al. (2012), in their corresponding research work on methods used by fraudsters confirmed Ifinedo's, (2012) findings that individuals' response to a threat depends on their perception of the threat riskiness and their willingness to accept the threat. There have however been several isolated research works focusing specifically on identity flexibility, dissociative anonymity, and intermittent cyber ventures socially engineered cyber deception and theft (Danquah, Longe & Totimeh, 2012; Febriana & Fajrianthi, 2019; Suler, 2004; Koranteng, Apau, Opoku-Ware & Ekpezu, 2020). Generally, it is evident in most findings that worth of the security of users' information assets is certain, secured systems upturns users' integrity and reputation.

In Jaishankar (2008), the influence of identity flexibility and dissociative anonymity was not decoupled from the lack of a deterrence factor, the implication is that internet-based security is yet to develop the capability of users being deterred by the presence of deterring visibility (online/cyber police). As mentioned earlier, the totality of one's self-construal and the ability of the individual to modify either partly or fully the self-construal and yield to its actual when needed is essentially identity flexibility (Weinreich, 1986). The dissociative anonymity depicts states in which an individual's identity is unknown and also detached from the individual or environment (Wallace, 1999).

In structured environments such as corporate organizations, the Security Operations Centre (SOC) is usually used as base for identifying breaches, performing triage, containment, and escalation (Danquah, 2020). Environments of this nature leverage on frameworks to guide the management of various forms of cybercrime.

## METHODOLOGY

This research used a predominantly qualitative approach with some quantitative descriptive statistics in addition. The qualitative component was mainly interviews which involved collecting non-numerical data to understand concepts, opinions, or experiences on the subject matter. This was complemented by an experimental website which was used to collect quantitative data, this involved collecting and analysing data numerically to serve as compliment and validation the qualitative data.

In view of the potential of a relatively small sample size being seen to threaten the validity and generalizability of this study, the preferred perception of Green and Thorogood (2004) was considered. Specifically, they explained that qualitative researchers conducting an interview-based study are likely to generate a little new information with more subjects or numbers (pp. 102–104). This is further confirmed by Ritchie et al. (2003). Qualitative research experts argue that there is no straightforward answer to the question of 'how many' and that sample size is contingent on a number of factors relating to epistemological, methodological, and practical issues Baker, Edwards & Doidge (2012, pp.29). In view of these assertions, this research is extended beyond just the interviews to have an experimental component to be more transparent about evaluations, improve sample size sufficiency, and ultimately situate these within a broader and more encompassing assessments of data adequacy.

Article DOI: https://doi.org/10.37284/eajit.5.1.673

With the postulate in Space Transition Theory as the foundation, the derived identity flexibility and dissociative anonymity provides a basis for any arguments. The objective of this research work could best be accomplished via a qualitative approach because of the provision of in-depth understanding of this methodology. Following this approach, the case study was deemed appropriate. According to Yin (1994, p. 13) the case study method is "an empirical enquiry that investigates a contemporary phenomenon within its real-life context especially when the boundaries between phenomenon and context are not clear". The qualitative approach of case study was consequently used for this study. A qualitative approach of interviews and an experiment are used for data collection. The interviews were carried out with four victims of internet fraud and three culprits of internet fraud upon obtaining clearance from the Ghanaian police Service to conduct the ethnographic study. Inclusion criteria of research participants was based on availability for interviews and the contextual application of the interviewee's response. This essentially, therefore, focused on Ghana for data via interviews.

Additionally, a researcher developed website was also hosted to serve as a honey bait to profile all site visitors with specific interest in knowing whether visitors would attempt to access and obtain illegal content with authentic identity. Though the website displayed a disclaimer, there was a popup on the site's homepage to indicate that activities of users may be logged for research purposes.

The site required users with criminal intent to register by providing credentials about themselves which were validated using phone numbers and emails. The credentials of users were used to ascertain their authenticity. The website was designed using HTML, PHP with embedded SQL scripts and hosted on a Linux server running Apache as the webserver and MySQL as the database.

Participants were recruited via e-mails to mailing lists, and advertisement on various social media sites. To successfully track site visitors, three monitoring tools namely Webalizer, AWStats, and self-developed tracking tools were used.

The specific components/links of the site included access to the Home, News, Academics, Inspiration, Shareware and Disclaimer, Usable Credit Cards, Pornography (child), Software Cracks, Stolen Passwords, Games Download, and Registration. The non-crime related links were "Home, News, Academics, Disclaimer and Inspiration" whereas "Shareware, Usable Credit Cards, Pornography (child), Software Cracks, Stolen Passwords, and Illegal Games Download" were considered to be the crime related links.

Hyperlinks to unlawful content were not legitimate hence non-functional; they only required interested users to register for access to more details, after which the information "try next time" message was displayed to users. The links to lawful material were on the other hand legitimate and essentially provided users with the appropriate information displayed. Analysis of data for both interviews and results from the experimental website were done using a content analysis approach.

The various sources of evidence helped to reduce the potential bias of the single method (Bowen, 2009). This increases the credibility of the findings and the relative importance of the conclusions drawn from the analysis (Eisner, 1991).

## RESULTS

### Paraphrased Victims' Responses

For the purpose of protecting the identity of the victims, pseudo names have been used in the cases described below.

#### *The Case of Michael*

Michael a retired construction worker from Australia met Sarah on www.afrointroductions.com and developed a romantic love relationship with her over a six-month period. During the relationship building process they used an online chat service, e-mail, telephone and occasionally webcam chats to communicate. Upon building some level of trust, Michael started remitting Sarah on a weekly basis an average of $5000, this continued for over four months. The two then agreed to get married, in the process Sarah's family made a laudable gold business proposal to Michael, this required Michael to transfer about $60,000 to successfully transact the business and supposedly reap huge financial benefits afterwards. The intention was for Michael

Article DOI: https://doi.org/10.37284/eajit.5.1.673

to follow up with a trip to Ghana to settle down with his new wife, Michael therefore transferred the money to a foundation account and followed up with a trip to Ghana. It turned out that he was virtually deserted by Sarah and her family upon arrival, much as he met the supposed Sarah; she strangely had to travel out of Ghana at the same time. Upon suspicious observations made by Michael and the advice of his embassy in Ghana, Michael was assisted by the police to use a bait to arrest the suspects. It turned out that the supposed Sarah was not real and had been hired temporarily for live webcam chats by a sophisticated syndicate.

***The Case of Madam Denise***

Denise received a text notifying her of a prize she had won, the text requested that she sends funds to another number to make her eligible to collect her prize which was some thousands of Ghanaian cedis. She complied and ended up sending credit to this other number to the tune of about GHC150 Ghana cedis or the equivalent of $100. It was not until her daughter called the telecom company to inquire about the authenticity of the text message that she realized it was a scam.

***The Case of Phyllis***

Phyllis is a British accountant who was swindled through a dating website which involved sending money to an individual in Ghana without adhering to an original agreement. The fraudster was supposed to pay the money back upon arrival at Britain after having had over $15,000 in seven (7) transfer transactions. The culprit claimed to be an Australian researcher based in London but happened to be working in Ghana and in conjunction with the Ghanaian government in his research. Phyllis communicated with the supposed Australian in United States over the Internet, phone, and text messages. Subsequent investigation proved that all e-mail communication was from Ghana even when the culprit claimed to be in the United States. The implication is that the calls she even made to a genuine United States number were diverted to Ghana as well.

***The Case of Mary***

Mary is an American business woman who intended settling into a new life with her new found internet lover and was defrauded of $80,000. The relationship with a supposed retiring American military man developed via phone, text messages, and internet chat after meeting on a dating website. They planned to use the money to prepare a New York house for Mary to move in. They were supposed to meet up and perhaps commence future together, and it turned out the funds were transferred to a Ghanaian cedi bank account. With the aid of the bank's employee, the amount was withdrawn in 3 tranches by the fraudsters. Mary explained that the Colonel claimed he was part of the soldiers withdrawn by the United States government from Afghanistan and was to take care of some properties wrongly shipped to Accra and would return to United States in two weeks. Whilst in Accra, the military man purportedly experienced some problems with the police and required part of the amount to resolve the issues and channel the residual to their intended property in the United States as agreed by the two of them. He requested that the money be paid to his lawyer who was impleading the case for him. Mary upon cross-checking from the Fraud Department of the United States confirmed the existence of the account in Ghana before she transferred the money into an account at reputable bank in Ghana. With aid of the bank's staff, the amount was withdrawn in 3 tranches. Mary never heard from the military man from that moment onwards and decided to take legal action against the bank for not doing enough due-diligence before the money was withdrawn.

**Paraphrased Response from Culprits**

***The Case of Dodoo***

Interview with Dodoo: Dodoo at the time, was a final year University student, studying Information Technology.

> *Question: How are you able to successfully gain access to credit cards?*

*Answer:* There is a payment service called liberty reserves, I usually pay money into a liberty account and then I use the reserves in the liberty account to pay for services of hackers who can gain access to the credit card details. When I register with liberty, I am provided with a login, password, and the master key which is the identification number of my

Article DOI: https://doi.org/10.37284/eajit.5.1.673

liberty card. This payment service can be used to conduct legitimate business payments, it just so happens that a lot of the online scammers are the ones who use it.

*Question: Once you pay for the hacking services and successfully obtain the credit card details, how do you purchase items and ensure you have received them?*

*Answer:* The key is finding someone you can trust; you need to have built a relationship with that person to establish that trust. When the items are purchased, they are delivered at that person's address and then it is subsequently mailed to you here in Ghana. In Ghana it is important to also have an insider at the port who will assist you with clearing without you being indicted. Most of the time you do not have to use your real name to obtain the items.

*Question: When you communicate with the hackers and also make purchases online, do you do that directly from your PC or you use proxy servers?*

*Answer:* No, I do not go directly, there are tools like "hide my ass" and "anchor" which enable you change your IP address to make it seem as if you are from another country or even sometimes unknown. Once you make the change, you can confirm by accessing a site like "whatismyip.com" to confirm the change.

***The Case of Yaw***

Yaw is a university student who was also quite open with providing information about his activities. He therefore granted an interview of which the salient responses are transcribed below. He comes from a seemingly disciplined background with a very keen interest in technology. He is an IT student in his final year at the University. He came across as quite sincere with his responses; he did not hesitate at all.

*Question: How have you been successful in internet fraud activities?*

*Answer:* I first had the idea when I learned about key loggers and what they could be used for, I became curious and one thing led to another. I must say that I am not into defrauding people online. I search for usable credit card numbers online and use them to purchase downloadable (soft copy) products like books, journals, movies, and music. I cannot be sure of delivering a tangible item to a physical address somewhere. It may put the recipient in trouble hence I use my online identification.

*Question: What exactly do you do to get access to these credit card numbers?*

*Answer:* You go online and search for credit card numbers, one key word that has been very helpful is "discard". Once I am successful in finding some numbers, I then need to look for a valid address to be used for the card. On the average, if I find 10 card numbers and five valid addresses, I am able to shop satisfactorily. There are different types of cards like Visa, Master Card, and Discovery etc. They all have specific sites where they are usable and vice versa.

*Question: How sure are you that no one knows you are being tracked and could be arrested?*

*Answer:* I make sure I always cover my tracks by using a proxy server most of the time. I know those servers usually go out as anonymous, but I sometimes have to resort to a direct access since the proxy does not seem to be accepted by all websites.

*Question: You mentioned key loggers, what about it? Tell me how you use them.*

*Answer:* Well, I know some Internet Cafes use them to obtain vital information for accessing people's accounts. I just happen to know how it works but I have never used it to collect anyone's confidential information.

*Question: Have you defrauded any other person before?*

*Answer:* Yes, I have defrauded several others

*Question: Do you use the same or real identity and how do you manage your identity?*

*Answer:* I sometimes use the same identity but never my real identity, I have a number of different identities I use on different platforms. I try to change as and when I find it necessary.

Article DOI: https://doi.org/10.37284/eajit.5.1.673

***The Case of Solo***

The Case of Solo is a second year University student who was quite open with providing information about his activities. He is a very resourceful technical IT person. Having worked several years in the industry, he decided to pursue a degree program but admitted to being involved in cyber deception and theft. He therefore granted an interview of which the salient responses are transcribed below;

*Question: How have you been successful in internet fraud activities?*

*Answer:* We first of all go to the internet, search for a client via chat rooms, e-mail messages, social sites to random addresses etc. When they reply then you try to build a relationship with the person, and establish trust. I usually buy them phones, ladies wear for the ladies etc. Building this relationship takes time, for me sometimes it takes up to six months. Get the victims contact details like e-mail address and other credentials to the hackers.

*Question: Who are the hackers and how do you get access to them?*

We pay hackers for their services, for them, their work ends after they hack and provide you with banking information and requisite credentials for banking online or credit card details. They can be found on some specific websites; these sites change very often and on the fly. For instance, you can now find them on ccdan.org, ccfucke.org and ndan.co.cc/1. These sites would not be accessible in about a week's time for their security reasons. Besides, the hackers do not respond to everyone's request unless you are introduced by their trusted colleague. We have some leads but I cannot tell you. Sorry about that. The hacker accesses the victim's e-mail address and attempts to find out much about the victim, mainly their financial standing and bank details to enable me (the culprit) here carry out some bank transfer. I have some contacts there (abroad) whose accounts are used. I also have to pay them for their services before finally the money is transferred to me here. To build trust, you need a liberty account, it is like PayPal. They have agents at some places like Busy Internet here in Ghana. It is my money in the liberty account that I use to make payments for little things like gifts for my eventual victim and the hackers. Once I have access to the victims' credit card details, I test it to determine how much I can spend by trying to purchase some items, it could range from laptop, booking a flight to attempting to even buy a car. That gives you an idea of how much money you can spend, but do not complete the transaction. One other important fact about the credit card information is that, they mostly restrict the usage of the credit cards to specific websites. For the credit cards, there are different types; e.g., Discovery, Diana, and American Express cards are usually expensive at least $100 whiles others like Visa and Master Card are relatively cheap. Gaining access to the hackers for their services is not an easy task. You must be introduced by someone who is already in the business for a hacker to patronize you. Firstly, before the hacker helps you in any way, they will hack your e-mail address and review your e-mail communication before they decide whether it is safe to do business with you or not. To really make money, you must work with others to enable you beat the system. I have been successful on countless occasions, but when the goods are arriving here in Ghana, it is extremely critical that you work with an insider at customs. Also, you do not always need to use a real identification, you must use a fake identification card else you can be tracked.

*Question: Have you defrauded any other person before?*

*Answer:* Yes, I have defrauded three other people

*Question: Do you use the same or real identity and how do you manage your identity?*

*Answer:* I have my fake online account which has a totally different identity and phone number connected. I try to create a new one about every three to four months.

***The Case of BKS***

BKS is a second year University student who was quite open with providing information about his activities. He is a relatively new person to the technical Information Technology field. He decided to pursue a degree program out of interest for the field and admitted to being involved in cyber deception and theft. He came across as very open and honest with his responses. He therefore granted

Article DOI: https://doi.org/10.37284/eajit.5.1.673

an interview of which the salient responses are transcribed below.

*Question: I am aware you do a lot of credit card hacking and usage online, how exactly do you get it done?*

*Answer:* I either access a website that sells credit cards or I use a hacker to provide me with the needed credit card and the details. I usually use the hacker; I get access to the hacker through the internet sites like the hackers' lounge at www.yahoo.com etc. One essential requirement from our part of the world is to have a liberty reserve, this is an online account that enables one to make payments for services rendered by the hackers. Once you have successfully stashed your liberty account with the money needed, then you purchase the credit card from the hacker with money in that account. Prices of the cards vary depending on what type of credit card you intend to buy. American Express and Discovery are the relatively expensive cards, cards like Mastercard and Visa are usually fairly moderate in price. You can also access site like www.cardexstore.com to purchase a credit card, again you may have to pay with liberty reserves, that is more reliable but the sites really change often. There is a network of dealers who circulate the new site addresses to each other.

*Question: How do you successfully receive the items you buy with the credit cards?*

*Answer:* Usually, you must have developed a relationship with someone you can trust, you can then use the person's address as the receiving address of the items purchased. The person then in turn would send the items to you. Usually, it is not safe for you to receive the items in person so you have to work it out with some custom official. A few times I have picked up the items myself. Take note, the supposed friend who sends you the items must be someone with whom you have built a friendship of trust over a period. That is usually done by buying the individual presents occasionally over a long period like six months and over. One other thing, some of the credit cards are what is called "verified by data", those ones usually have passwords and payment with those are usually declined. It is important you know these so you do not choose the wrong type.

*Question: How much do you usually pay for the credit cards?*

*Answer:* About $3 to $5 per credit card. Some of the sites expect you to register, those ones usually charge $50 and over before they provide any services.

*Question: Have you been successful in this endeavour?*

*Answer:* I have been able to purchase a lot of items with the use of this method, I have purchased laptops, iPad, even my shirt and slippers.

*Question: What tools or software do you use to assist you with this endeavour?*

*Answer:* Well, before you can hack or buy something online, you must get a VPN and a very strong one, you need to hide your identity or location by going to vpn.com or hidemyass.com to change your IP address to make it reflect as if you are in the US or some other part of the world.

*Question: Have you ever been successful not going through the proxy server, I mean going directly to buy items online?*

*Answer:* No, the system will not allow you

*Question: Have you defrauded any other person before?*

*Answer:* Yes, I have defrauded a few other people

*Question: Do you use the same or real identity and how do you manage your identity?*

*Answer:* I never use my real identity. That is the first rule to be successful in this our business. I use false multiple identities but I have my connections where the money is collected hence, I still get to collect my money whenever I need to. I change or create new identity as and when it is necessary.

**Results from Experimental Website**

This section is focused on results from the experimental website, these include summary of access to experimental website, distribution of duration of visits to experimental website, summary of user agents (browsers) used to access

Article DOI: https://doi.org/10.37284/eajit.5.1.673

experimental website and distribution of accessed links on experimental website. Additionally, this section details the distribution of registration link access and analytical distribution of user access and registrations. This section presents results intended to complement the qualitative data collected via interviews by presenting results from an experimental website which was used to collect quantitative data.

Unique session identification numbers used to track individual click patterns and user activities on the website where as registration tally is established on distinctive user credential accounts. This measure assured that different users could not register more than once using different identifications. The total statistics was generated by the three monitoring tools used for the data collection presented varying numbers. The developed tracker was the sole tool that was used to track the specific links accessed as well as their respective unique session identification numbers.

The method of recruiting participants was via e-mail and various social media sites. This may have caused a skew in the results.

Below in *Figure 2* and *Tables 1, 2,* and *3* is a comparative summary of access obtained from the hosting service provider's analytic tool, it shows a total of 135 visits to the site from the Webalizer tool and 196 visits from the AWStats tool in the table. 64.29 percent of users spent less than 30 seconds on the site with 15.8 percent of visitors spending between 30 second to 2 minutes on the site. 10.71 percent of the users spent 2 to 5 minutes on the site and the remaining 9.18 percent spent 5 to 15 minutes on the site. 70 percent of users used the Google Chrome browser to access the site whereas 5 percent and 2.50 percent used Mozilla and Safari browsers respectively. The tools were unable to detect 22.50 percent of browsers used to access the site.

**Figure 2: Summary of Access to Experimental Website**

**Summary by Month**

| Month | Daily Avg. | | | | Monthly Totals | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Hits | Files | Pages | Visits | Sites | KBytes | Visits | Pages | Files | Hits |
| May 2021 | 1 | 1 | 1 | 1 | 18 | 96 | 25 | 25 | 26 | 26 |
| Apr 2021 | 1 | 1 | 1 | 1 | 21 | 141 | 30 | 42 | 50 | 50 |
| Mar 2021 | 0 | 0 | 0 | 0 | 9 | 32 | 16 | 16 | 16 | 16 |
| Feb 2021 | 0 | 0 | 0 | 0 | 8 | 27 | 14 | 14 | 15 | 15 |
| Jan 2021 | 1 | 1 | 1 | 1 | 21 | 123 | 31 | 32 | 37 | 37 |
| Dec 2020 | 0 | 0 | 0 | 0 | 3 | 9 | 10 | 10 | 10 | 10 |
| Nov 2020 | 0 | 0 | 0 | 0 | 4 | 9 | 6 | 6 | 6 | 6 |
| Oct 2020 | 2 | 2 | 2 | 1 | 3 | 18 | 3 | 4 | 4 | 4 |
| **Total** | | | | | | **455** | **135** | **149** | **164** | **164** |

Source: Webalizer

**Table 1: Distribution of Duration of Visits to Experimental Website**

| Duration of Access | Number Recorded | Percentage |
|---|---|---|
| 0s-30s | 126 | 64.29% |
| 30s-2mn | 31 | 15.82% |
| 2mn-5mn | 21 | 10.71% |
| 5mn-15mn | 18 | 9.18% |
| 15mn-30mn | 0 | 0.00% |
| 30mn-1h | 0 | 0.00% |
| 1h+ | 0 | 0.00% |
| | 196 | 100.00% |

Source: AWStats

Article DOI: https://doi.org/10.37284/eajit.5.1.673

**Table 2: Distribution of User Agents (Browsers) Used to Access Experimental Website**

| Browser | Percentage |
|---|---|
| Google Chrome | 70% |
| Unknown | 22.50% |
| Mozilla | 5% |
| Safari | 2.50% |

Source: AWStats

The self-developed tracking tool turned to record generally higher figures than the tools provided by the hosting platform, emphasis for tracking was on the registration for the purpose crime or fraud related activities. Below is a distribution of the clicks as a result of intended registration via specific links and the actual successful registrations completed. This depicts that only 0.051 percent of intended registrations were eventually completed.

**Table 3: Distribution of Accessed Links on Experimental Website**

| Links | Registration Hits | Successful Registrations |
|---|---|---|
| Academics | 23 | 1 |
| Disclaimer | 1 | 0 |
| Games Download | 10 | 1 |
| Home | 72 | 0 |
| Inspiration | 4 | 0 |
| News | 10 | 0 |
| Pornography | 28 | 4 |
| Shareware | 11 | 0 |
| Software Cracks | 13 | 0 |
| Stolen Passwords | 5 | 0 |
| Usable Credit Cards | 19 | 4 |
| | 196 | 10 |

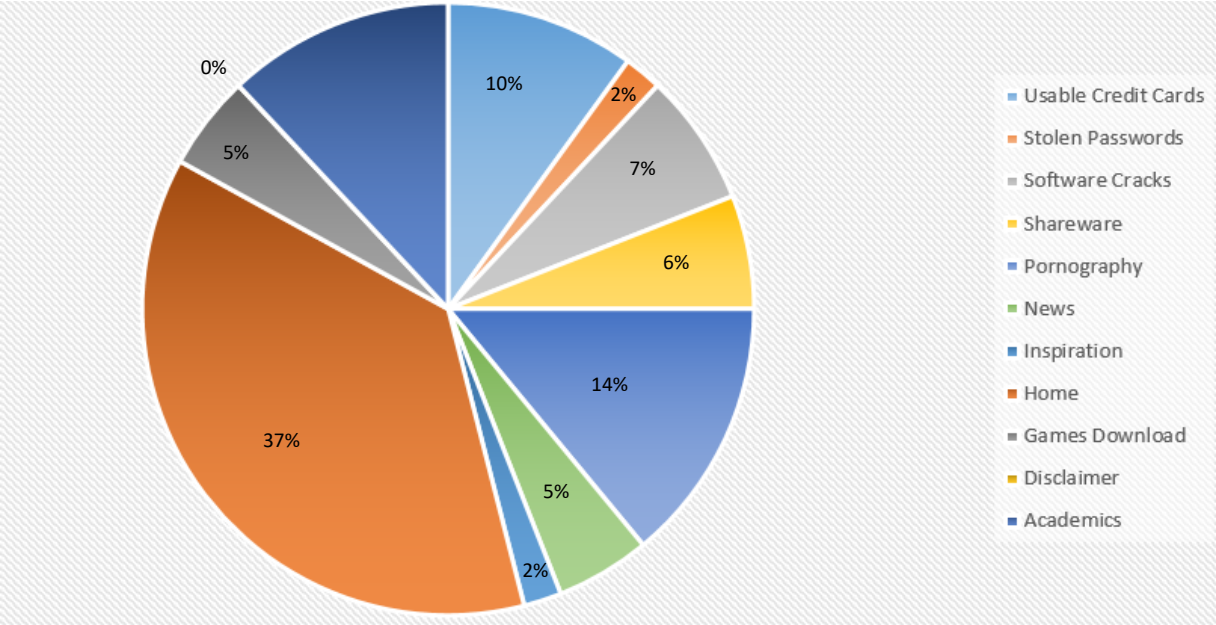
Source: Self-Developed Tool

Furthermore, 40 percent of completed registrations turned out to be as a result of interest in pornographic material and access to illegal usable credit cards. The remaining 20 percent was split equally between interest in academic material and games download.

Article DOI: https://doi.org/10.37284/eajit.5.1.673

**Figure 3: Distribution of Registration Link Access**




Source: Self-Developed Tracking Tool

For the purpose of this research where the focus is on identity flexibility and anonymity, a further analysis shows that despite the numerous accesses to the registration links for the purpose of obtaining information or material, some users accessed the registration link multiple times. In view of the validations implemented to ensure same users were unable to register multiple times via the same link, it was identified that there were 3, 1, 15 and 2 users for academics, games download, pornography, and usable credit cards respectively as shown in *Table 4* below. Further validations to determine the authenticity of their submissions also show that all entries made for registration via respective links were authentic.

**Table 4: Analytical Distribution of User Access and Registrations**

| Links | Registration Hits | Unique Users | Successful Registrations | Authenticity of Credentials |
|---|---|---|---|---|
| Academics | 23 | 3 | 1 | Yes |
| Games Download | 10 | 1 | 1 | Yes |
| Pornography | 28 | 15 | 4 | Yes |
| Usable Credit Cards | 19 | 2 | 4 | Yes |

## ANALYSIS AND DISCUSSION OF FINDINGS

The findings suggest that anonymity of culprits in terms of identity is further masked in some instances by false locations as their place of abode or source of communication. This was evident in the use of proxy servers and virtual private network connections. Additionally, it is unclear the reason for numerous unknown agents used to access the experimental website. The user identification and respective session identification numbers were however used to validate users to ensure unique identification. In view of the numbers recorded for unique users being 3, 1, 15 and 2 for academics, downloads, pornography, and cards respectively, it evident that users typical execute their ultimate intentions after several visits and attempts to the target.

Article DOI: https://doi.org/10.37284/eajit.5.1.673

Inferences via the responses obtained from victims, culprits, and the experimentation depict seemingly same pattern for all sources of data. Victims were defrauded by culprits who clearly practiced the application of identity flexibility and dissociative anonymity in their illegal endeavours. Despite the authenticity of registered crime related users on the experimented website, the true/actual identity of users cannot be confirmed even though their credentials were technically validated before being saved.

Responses from the culprits suggest that they make a conscious effort to satisfy all the requirements of any platform used but without necessary genuine credentials. Findings ultimately confirm the theoretical postulate by Jaishankar (2008) which states that "identity flexibility, dissociative anonymity and lack of deterrence factor in the cyberspace provides the offenders the choice to commit cybercrime". The other essential component which could not be implemented in the experimental website was the deterrence factor. This must be researched to further confirm the postulate in the routine activity theory that "the absence of a capable guardian" must be prevalent for the commission of a crime to be successful as also stated in the space transition theory. Future research must emphasize on development of solutions that serve as a reliable check on authenticity of users as well as deterrent to all fraudulent users.

## CONCLUSION AND RECOMMENDATIONS

This study investigated the influence of identity flexibility and dissociative anonymity on internet fraud, focusing on the cyber deception and theft. Using a predominantly qualitative approach of interviews and an experimental website, a content analysis of interview transcriptions and results obtained from experimental website were used to derive meanings from the collected data. This finding from this research work showed that victims of internet fraud were defrauded by culprits who applied identity flexibility and dissociative anonymity in their illegal endeavours.

Findings shown in the study confirm the theoretical postulate that "identity flexibility, dissociative anonymity and lack of deterrence factor in the cyberspace provides the offenders the choice to commit cybercrime" and consistent with existing studies. This study provides some recommendations to practitioners and future researchers for fraud prevention on the internet with emphasis on development of solutions that serve as a reliable check on authenticity of users as well as deterrent to all fraudulent users.

## REFERENCES

Baker, S. E., Edwards, R., & Doidge, M. (2012). How many qualitative interviews is enough? Expert voices and early career reflections on sampling and cases in qualitative research. *National Centre for Research Methods Review Paper*. http://eprints.ncrm.ac.uk/2273/4/how_many_interviews.pdf. Accessed 17 May 2018

Barlett, C. P. & Gentile, D. A. (2014). Predicting Cyberbullying from Anonymity, Psychology of Popular Media Culture. *American Psychological Association*, 5(2), 71–180, 2160-4134/16/http://dx.doi.org/10.1037/ppm0000055

Brenner, S. W. (2009*). Cyberthreats: The Emerging Fault Lines of the Nation State.* Oxford University Press. ISBN 9780190452568.

Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative Research Journal,* 9(2), 27-40.

Danquah, P. (2020). Security Operations Centre: A Framework for Automated Triage, Containment, and Escalation. *Journal of Information Security,* 11, 225- 240. https://doi.org/10.4236/jis.2020.114015

Danquah, P., Longe, O. B., Lartey, J. D., & Tobbin, P. E. (2020). Towards a Theory for Explaining Socially-Engineered Cyber Deception and Theft. In *Modern Theories and Practices for Cyber Ethics and Security Compliance* (pp. 44-58). IGI Global.

Danquah, P. (2015). *An Assessment of Cyber Criminal Behavioural Patterns* (PhD Thesis). Accra Institute of Technology Institutional Repository.

Article DOI: https://doi.org/10.37284/eajit.5.1.673

Danquah, P. & Longe, O. B. (2011). Cyber Deception and Theft: An Ethnographic Study on Cyber Criminality from a Ghanaian Perspective. *Journal of Information Technology Impact*, 11(3), 169–182.

Danquah, P., & Longe, O. B. (2011). An Empirical Test of the Space Transition Theory of Cyber Criminality: The Case of Ghana and beyond. *African Journal of Computing and ICT*, 2(2), 38–48.

Danquah, P., Longe, O. B., & Totimeh, F. (2012). Just another Harmless Click of the Mouse? An Empirical Evidence of Deviant Cyber Space Behaviour Using an Online Trap. *African Journal of Computing and ICT,* 5(3), 49–56

Danquah P. & Longe, O.B (2013). Towards a Framework for Evaluating Behavioral Patterns

of Cyber Criminals. *Proceedings of the iSTEAMS International Multidisciplinary Conference*, Conference Centre, University of Ibadan, Ibadan, Nigeria pp 217 – 226

Eisner, E. W. (1991). *The Enlightened Eye: Qualitative Inquiry and The Enhancement of Educational Practice*. Toronto: Collier Macmillan

Febriana, S. K. T. & Fajrianthi (2019), Cyber Incivility Perpetrator: The Influenced of Dissociative Anonimity, Invisibility, Asychronicity, and Dissociative Imagination, *Journal of Physics, Conference Series*, Volume 1175, 1st International Conference on Advance and Scientific Innovation, Medan, Indonesia

Green, J. & Thorogood, N. (2004). *Qualitative methods for health research*. London: Sage.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behaviour and the protection motivation theory. *Computers & Security*, 31(1), 83–95. doi:10.1016/j.cose.2011.10.007

Jaishankar, K. (2008). Space Transition Theory of Cyber Crimes. In F. Schmalleger & M. Pittaro (Eds.), *Crimes of the Internet* (pp. 283–301). Upper Saddle River, NJ: Pearson-Prentice Hall.

Koranteng, F. N., Apau, R., Opoku-Ware, J., & Ekpezu, A. O. (2020). Evaluating the Effectiveness of Deterrence Theory in Information Security Compliance: New Insights from a Developing Country. In *Modern Theories and Practices for Cyber Ethics and Security Compliance* (pp. 140-151). IGI Global.

Longe, O. B., Danquah, P., & Ebem, D. U. (2012). De-Individuation, Anonymity and Unethical Behaviour in Cyberspace – Explorations in the Valley of Digital Temptations. *Computing Information Systems Journal*, 16(1), 46-55

Ritchie, J., Lewis, J. & Elam, G. (2003), Designing and selecting samples. In: J. Ritchie & J. Lewis (Eds). *Qualitative research practice: a guide for social science students and researchers*. London: Sage. p. 77–108.

Suler, J. (2004). The Online Disinhibition Effect. *Cyberpsychology & Behavior*, 7(3), 321-326.

Wada, F., Longe, O., & Danquah, P. (1970). Action speaks louder than words-understanding cyber-criminal behavior using criminological theories. *The Journal of Internet Banking and Commerce*, *17*(1), 1-12.

Wallace, P. (1999). *The Psychology of the Internet*. New York, NY: Cambridge University Press.

Yin, R. K. (1994). *Case Study Reseach: Design and Methods* (2nd ed., Vol. 5). London: Sage Publications.