



INTERNET FRAUD AND INFORMATION NEEDS AND SEEKING BEHAVIOR OF INTERNET USERS IN DELTA STATE UNIVERSITY, ABRAKA

Dorcas Fibikah Otaru

Department of Library and Information Science,
Ignatius Ajuru University of Education, Port Harcourt
dorcasfibikahotaru@gmail.com

Prof. Anthonia E. Omehia

Department of Library and Information Science,
Ignatius Ajuru University of Education, Port Harcourt
anthonia.omehia@iaue.edu.ng

Abstract

The study investigated Internet Fraud and Information Needs and Seeking Behavior of Internet Users in Delta State University. Descriptive survey design was used for the study. The population of the study comprised internet users both students and staff in Delta State University. Accidental sampling was used to select 158 respondents. Questionnaire was used to collect data. Data collected were analysed using the descriptive statistics of arithmetic mean and standard deviation. The study identified identity theft fraud, online-investment fraud, admission fraud and others as the major forms of fraudulent activities. In order to be safe from these, the found that internet users need information how to identify a fraudulent activity online, genuine & reliable websites and databases, online information literacy, use of social networks, cyber security information. In the course of seeking information, internet users exhibit certain behaviours by viewing podcast & comments of victims online, checking comments of users on posted images and videos online, interacting with other trusted users. Lack of awareness on the existence of internet fraud, the rising role of technology on daily basis and others stand as the major barriers. Therefore, the study recommended the need for proper sensitization on the use of internet sites and social networks as well as adequate training on new technologies, and online information literacy skills among internet users.

Keywords: Internet fraud, Information needs, Seeking behaviour, Internet users

Introduction

Internet today is one of the greatest inventions in the whole wide world. It has provided an avenue as well as a backbone for electronic commerce, research, communication, and education both in the developing countries and the developed. Students and staff in various universities often engage in internet search for pertinent information and communications through the use of social networks, Google search engine, electronic mail, and voice communication devices such as skype, zoom, etc, integrated into higher learning institutions for effective interactions, reflection of learning, quality of teaching and students' academic performances (Okeke & Nsirim, 2024). The use of internet for one reason or the other is



increasing on a daily basis and the presence of unlimited internet connectivity across universities often results in students and staff spending considerable amounts of time online. Apart from it being the greatest inventions, it is also regarded as a killer application, as the risks of using internet are becoming unendurable due the increasing number of its illegitimate users otherwise known as fraudsters on a daily basis.

The term ‘internet fraud’ refers to any type of fraud scheme that uses email, web sites, chat rooms or message boards to present fraudulent solicitations to prospective victims, to conduct fraudulent transactions or to transmit the proceeds of fraud to financial institutions or to others connected with the scheme (Australian Federal Police, n.d). Internet fraud is not considered a single, distinctive crime but covers a range of illegal and illicit actions that are committed in cyberspace. Its forms may include spam, scams, spyware, identity theft, phishing or internet banking fraud. In 2018, the FBI’s Internet Crime Complaint Center reported figures that show Internet-enabled theft, fraud, and exploitation being responsible for \$2.7 billion in financial losses (FBI 2018). According to Button et al. (2016) also reported that Internet-based fraud as the fastest growing crime in the UK in 2015–2016, with 3.25 million victims each year and an annual combined loss of £3.6 billion. Estimates show that 4.7 million incidents of fraud were experienced by adults aged 16 and above in England. The crimes are being influenced by the rising role of technology which made it difficult to always know the background of the perpetrators by the law enforcement community globally (Norris et al, 2019).

The challenge for university libraries today is how to meet the needs of Internet users in their search for information in a cost-effective way, and to ensure that the search strategies employed by clients are both efficient and return quality results that satisfy user requirements without falling prey to fraudsters. Norris et al (2019) lamented that the possibility of falling victim to fraud is always high especially if one is unaware of the existence of internet fraud. Many internet users may not know that the internet can be used to deceive and swindle them out of their money or even steal personal information. Many users also use the service without taking any precautions, especially on unsecured auction websites (Mohatar & Sierra-Cámara, 2007). Unrestricted use of some websites often leads users to other websites that participate in fraudulent activities thus exposing them to a risk of being scammed. A search for a particular textbook for instance could lead a student to an online auction website where the book is offered. Pressure from lecturers and need for a particular book can also lead an individual to buy it from the website exposing him/her to the possibility of being a victim of fraud (Hache & Ryder, 2011). Hence, information needs and seeking behaviour of internet users bearing in mind the presence of fraudsters in academic institutions becomes so aim of the study.



Statement of the problem

In the emerging electronic environment, knowledge about the information needs and seeking behaviour of internet users is crucial for those wishing to help them effectively meet their information needs online. Internet fraudulent activities today has increased the need for accurate and reliable information by internet users. In higher institutions, most users often fall victims and do not wish to use the internet anymore due to the fear of falling prey to fraudsters. Invariably, not using the internet is even more worse than its negative effects considering the amount of information resources in the cyberspace, rather, it demands that users should be conscious of the fraudulent activities online so as not to fall victims. In Delta State University, observations show that most fraudsters are involved in hiding of information or providing incorrect information for the purpose of tricking victims out of money and properties online. Some victims are made to provide their bank details and they empty their accounts in a minute. Based on the foregoing issues, the study therefore is set to identify the fraudulent activities and information needs and seeking behaviour of internet users in Delta State University.

Objectives

1. To identify the fraudulent activities among internet users in Delta State University
2. To identify the information needed by internet users to overcome fraudulent activities in Delta State University
3. To identify the seeking behaviours exhibited by internet users in overcoming fraud in Delta State University
4. To identify the problems affecting the seeking behaviours of internet users in Delta State University

Research Questions

1. What are the fraudulent activities faced by internet users in Delta State University?
2. What information are needed by internet users to overcome fraud in Delta State University?
3. What are the seeking behaviours of internet users in Delta State University?
4. What are the problems affecting the seeking behaviours of internet users in Delta State University?

Literature Review

The internet was known as ARPANET system, a military network established in the United States in the late sixties. The interconnection of computers is known as a network.



According to Wiche et al., (2024), internet is nothing but a network of networks or is a huge network of computers that links the different type of computers around the world. The internet has many user-friendly tools which help the users to interact with the internet and get the information they need. Some of these tools are Gopher, Archie, and World Wide Web (WWW). The internet is rich resource of information and provides the information to its users faster than any other resources. Therefore, it became the most popular resource of information where all seekers depend on. Despite the enormous benefits to internet subscribers, its use today is exposing people to many risks ranging from identity theft, fraud, and exposure to malware that can easily result in harm to the users (Norris et al., 2019). Mostly the internet has created more room to fraudulent activities globally even in Nigerian universities.

Fraud is an act of wilful deception that produces an economic benefit (or evasion of a loss) for the deceiver and a loss for the victim either online, physical or both (Kemp, 2020). Internet fraud is a type of cybercrime fraud or deception which makes use of the internet and could involve hiding of information or providing incorrect information for the purpose of tricking victims out of money, property, and inheritance (Wikipedia). It also refers to any type of fraud scheme that uses email, web sites, chat rooms or message boards to present fraudulent solicitations to prospective victims, to conduct fraudulent transactions or to transmit the proceeds of fraud to financial institutions or to others connected with the scheme (Australian Federal Police, n.d). Internet fraud takes a number of forms with perpetrators currently relying on telemarketing, emails, and presenting themselves personally to unsuspecting people met in online chat rooms or social networks. Kemp (2020) identified online- investment fraud, charity fraud, relationship and trust fraud, identity theft fraud etc.

The most common form of online fraud occurs through sale or advertisements of goods and services that do not exist. In universities, students are more likely to fall prey as they have a desperate need for many products not sold locally. They end up giving away their credit card information to buy those products. Most of the time however, goods and services paid for are not delivered to the buyer. This common occurrence has seen many students and teachers lose money to fraudsters. Early detection is possible and can result in the reimbursement of funds if reported immediately to the bank issuing the credit or debit card (Brown, 2011). Another form of fraud comes in the form of phishing. This occurs when spam mails are sent to unsuspecting individuals. Scammers usually pretend to come from a company or organization that is well known. Phishing is soliciting personal information that can be used to steal an individual's identity as well as information related to banking that can result in loss of funds through credit card purchases that are unauthorized. One example of such an email is the recent



phishing done with the aim of getting individuals to divulge their PayPal account details (Chua, Jonathan, & Daniel, 2007). However, it is possible to fall victim if one is unaware of the existence of internet fraud, this is due to the common reason that most internet users may not know that the internet can be used to deceive and swindle them out of their money or even steal personal information (Mohatar & Sierra-Cámara, 2007). Therefore, information needs of internet users on fraud is imperative.

Information needs simply means the piece of information needed by a person or group of persons in order to satisfy a need. Ogbomo (2010) defined information needs as comprehensive information which makes it possible for the user to make proper judgment on any related problem facing him or her at a particular time. Wilson (2000) stated that information needs are determined by a number of factors such as the types of information sources available, purposes of the information, the background, motivation, professional orientation and individual characteristics of the user. The information needs of internet users vary, especially when they are online. Most internet users sometimes cannot possibly explain what exactly they want online. Omidian & Seifi-Maleki (2013) identified three needs for internet users to include: internet autonomy, competence, and relatedness support. Mohatar & Sierra-Cámara, (2007) also added that the internet users need information the existence of internet fraudsters and their approaches, this is due to the common reason that most internet users may not know that the internet can be used to deceive and swindle them out of their money.

Information-seeking behaviour begins when one realizes the existence of an information need and ends when that need is believed to have been satisfied. Especially, when an individual perceives that there is an information gap and tries to fill the gap to satisfy his information needs (Fatima & Ahmad, 2008). According to Singh, Kumar and Khanchandani, (2015) information seeking behavior can be defined as the attitude people portray when searching for information. This encompasses the feelings, actions, utterances, anger, anxiety, reluctance, zeal or any other attribute exhibited by an information seeker in his quest for satisfying his information need. They comprise of all the activities an individual engages in when trying to satisfy his information need. The internet users rely on the information gotten from web, especially when the information is from trusted sites.

Efforts have been made by both governmental and non-governmental organisations to educate individuals on the way in which criminals operate online on millions of these fraudulent activities (NAO 2017), but the inherent human weaknesses for incentive-driven behaviours seemingly make many of these scams too alluring to resist. For example, priming



individuals with images of money has been shown to reduce helpfulness towards others and increase isolation in tasks involving new acquaintances (Vohs et al. 2006). The rising role of new technology globally also influence the crime as users are not yet aware of their uses (Norris et al., 2019).

Methodology

The study examined Internet Fraud and Information Needs and Seeking Behavior of Internet Users in Delta State University. Descriptive survey design was used for the study. The population of the study comprised internet users both students and staff in Delta State University. Accidental sampling was used to select 158 respondents. Questionnaire was used to collect data. Data collected were analysed using the descriptive statistics of arithmetic mean and standard deviation. The decision rule for the mean was 2.5 which implies that items with the mean score of 2.5 and above are accepted and rejected if otherwise.

Analysis

Table 1: the fraudulent activities in Delta State University

The respondents were asked the various the fraudulent activities in Delta State University State.

Identify the forms of internet fraud in your school	$\bar{x}$	$\pm$	Decision
Phishing and Vishing fraud (identity theft fraud)	2.71	.732	Accept
Online-Investment fraud	3.82	.941	Accept
Admission fraud	3.92	.991	Accept
Course Sorting fraud	3.41	.931	Accept
Relationships and trust fraud	2.84	.701	Accept
Employment fraud	3.54	.841	Accept
Charity fraud	3.05	.804	Accept

Table 1 above shows the various fraudulent activities that exist among internet users in Delta State University. According to the respondents as represented in the table, the following were accepted as the major fraudulent activities in university understudy as the mean scores were above 2.5 based on the decision rule. Therefore, the activities include: identity theft fraud ($\bar{x}$ =2.71), Online-Investment Fraud ($\bar{x}$ =3.82), Course Sorting fraud ($\bar{x}$ =3.41), Relationships and trust fraud ($\bar{x}$ =2.84), Employment fraud ($\bar{x}$ =3.54), Charity fraud ($\bar{x}$ =3.05), and Admission fraud ($\bar{x}$ =3.92). These fraudulent activities are worrisome among internet users, depriving them the joy from effective interaction and transactions in the cyberspace. This particular finding is in



corroboration with the study of Kemp (2020) on Fraud Against Individuals in the Internet Era: Trends, Victimization, Impact and Reporting.

Table 2: the information needs of internet users in Delta State University

The respondents were asked the information needs of internet users in Delta State University State.

Identify your information needs	$\bar{x}$	$\pm$	Decision
How to identify a fraudulent activity online	3.51	.842	Accept
Genuine & reliable websites and databases	3.93	.952	Accept
Online information literacy	3.12	.851	Accept
Internet autonomy and competence	2.91	.791	Accept
Use of social networks	2.64	.771	Accept
Precautionary measures of fraudulent act	2.54	.661	Accept
Cyber security information	3.67	.976	Accept

Table 2 above, shows the information needs of internet users in Delta State University State. According to the respondents as represented in the table, all items were accepted, as the mean scores are above 2.5 in line with the decision rule. This indicates that internet users need information on how to identify a fraudulent activity online ($\bar{x}=3.51$), Genuine & reliable websites and databases ($\bar{x}=3.93$), Online information literacy ($\bar{x}=3.12$), Internet autonomy and competence ($\bar{x}=2.91$), Use of social networks ($\bar{x}=2.64$), Precautionary measures of fraudulent act ($\bar{x}=2.54$), Cyber security information ($\bar{x}=3.67$). All these information needs when provided will protect internet users from falling prey to fraudsters.

Table 3: the seeking behaviours of internet users in Delta State University

The respondents were asked the seeking behaviours of internet users in Delta State University.

Identify the behaviours exhibited when seeking information	$\bar{x}$	$\pm$	Decision
Viewing podcast & comments of victims online	3.91	.932	Accept
Checking through comments of users on posted images and videos online	3.83	.942	Accept
Interacting with other trusted users	3.82	.921	Accept
Checking profiles of users	3.51	.891	Accept
Engaging in online group discussions	3.04	.801	Accept



Searching through google, wiki and other database for information	3.14	.841	Accept
---	------	------	--------

Table 3 above shows the summary of Mean Rating and Standard Deviation of the seeking behaviours of internet users in Delta State University. As represented in the table, all items meet the acceptance requirements and therefore accepted as their means are above 2.5 in-line with the decision rule. This indicates that their seeking behaviours were exhibited through: Viewing podcast & comments of victims online, Checking through comments of users on posted images and videos online, Interacting with other trusted users, Checking profiles of users, Engaging in online group discussions, Searching through google, wiki and other database for information. All these can result in spending a considerable amount of time online

Table 4: the problems affecting seeking behaviours of internet users in Delta State University?

The respondents were asked the problems affecting their seeking behaviours of in Delta State University?

Identify the problems that affect your seeking behaviour	$\bar{x}$	$\pm$	Decision
Lack of awareness on the existence of internet fraud	3.31	.812	Accept
The rising role of technology on daily basis	3.93	.952	Accept
Lack of skills on the use of the internet and social networks	3.82	.981	Accept
Desperateness among users	2.91	.791	Accept
Poor internet networks	3.04	.906	Accept
Unreliability of internet sources	2.54	.941	Accept
Information proliferation	3.15	.854	Accept

Table 4 above shows the problems affecting their seeking behaviours of in Delta State University. According to the respondents as represented in the table, that barriers affecting seeking behaviours include: Lack of awareness on the existence of internet fraud ($\bar{x}$ =3.31), The rising role of technology on daily basis ($\bar{x}$ =3.93), Lack of skills on the use of the internet and social networks($\bar{x}$ =3.82), Desperateness among users ($\bar{x}$ =2.91), Poor internet networks ($\bar{x}$ =3.04), Unreliability of internet sources ($\bar{x}$ =2.54), and Information proliferation ($\bar{x}$ =3.15). This is due to the fact that the means scores of all the items were above 2.5 and therefore accepted.



Conclusion

Fraud is now the order of the day as far as internet is concern, every day new methods to defraud people are being devised and this simply places people at a risk of falling prey to online fraud schemes. Knowing when one is a victim is an important and reporting to appropriate authority may really help. The study identified identity theft fraud, online-investment fraud, course sorting fraud, relationships and trust fraud, employment fraud, charity fraud, and admission fraud as the major forms of fraudulent activities in universities. Therefore, internet users need information how to identify a fraudulent activity online, genuine & reliable websites and databases, online information literacy, internet autonomy and competence, use of social networks, precautionary measures on fraudulent act, cyber security information as identified. In the course of getting information, internet users exhibit certain behaviours by viewing podcast & comments of victims online, checking comments of users on posted images and videos online, interacting with other trusted users, checking profiles of users, engaging in online group discussions, searching through google, wiki and other database for information. However, lack of awareness on the existence of internet fraud, the rising role of technology on daily basis, lack of skills on the use of the internet and social networks, desperateness, poor internet networks, unreliability of internet sources, and the proliferation of information form the barriers to their seeking behaviour.

Recommendations

Based on the findings of the study the following recommendations were made:

1. The university management, in collaboration with ICT units and security agencies, should implement continuous cybersecurity awareness campaigns and digital literacy workshops. These programs should educate students and staff on common online fraud tactics such as phishing, identity theft, impersonation, scholarship scams, and fake investment schemes. Regular monitoring and reporting mechanisms should also be established to detect and curb fraudulent activities on campus.
2. The university should provide reliable and timely information through verified channels such as official websites, university emails, library bulletin boards, and WhatsApp groups. This information should include practical tips on safe browsing, secure passwords, recognizing fraudulent messages, and how to verify online platforms before sharing personal or financial details. ICT centres and university libraries should create help desks or portals for cybersecurity guidance.



3. Training students on how to search for, evaluate, and apply online safety information will improve their ability to counter digital fraud. Peer education through campus ambassadors and student associations should also be encouraged.
4. The university should improve internet access, provide training on proper information search strategies, and create a confidential reporting system for fraud-related issues. Additionally, librarians and ICT staff should be equipped to support students in navigating online safety resources.

References

- Australian Federal Police. (n.d.). *Internet fraud*. <http://www.afp.gov.au/>
- Brown, E. (2011). Internet law in the courts. *Journal of Internet Law*, 12(7), 22–25.
- Chua, C. E. H., Jonathan, W., & Daniel, R. (2007). The role of online trading communities in managing internet auction fraud. *MIS Quarterly*, 31(4), 759–781.
- Fatima, N., & Ahmad, N. (2008). Information seeking behaviour of the students at Ajmal Khan Tibbiya College, Aligarh Muslim University: A survey. *Annals of Library and Information Studies*, 55(2), 141–144.
- Federal Bureau of Investigation. (2018). *Internet crime report 2018*. Internet Crime Complaint Centre. https://www.ic3.gov/media/annualreport/2018_IC3Report.pdf
- Hache, A., & Ryder, N. (2011). 'Tis the season to (be jolly?) wise up to online fraudsters: Criminals on the web lurking to scam shoppers this Christmas—A critical analysis of the United Kingdom's legislative provisions and policies to tackle online fraud. *Information & Communications Technology Law*, 20(1), 35–56.
- Kemp, S. (2020). *Fraud against individuals in the internet era: Trends, victimisation, impact and reporting* (Doctoral thesis). Universitat de Girona. <http://hdl.handle.net/10803/671164>
- Khongtim, J. (2006). *Information seeking behaviour on Internet: A review* [Conference paper]. INFLIBNET Centre, 4th Convention Mizoram University, Aizawl, Ahmedabad.
- Mohatar, O., & Sierra Cámara, J. M. (2007). New directions in online fraud. *AIP Conference Proceedings*, 963(2), 973–976.



National Audit Office. (2017). *Online fraud*. National Audit Office.

Nikitkov, A., & Bay, D. (2008). Online auction fraud: Ethical perspective. *Journal of Business Ethics*, 79(3), 235–244.

Nkomo, N. (2009). *A comparative analysis of the web information seeking behavior of students and staff at the University of Zululand and the Durban University of Technology* (Master's dissertation). Department of Information Studies, University of Zululand.

Nkotagu, G. H. (2011). Internet fraud: Information to teachers and students. *Journal of International Students*, 1(2), 72–75. <https://doi.org/10.32674/jis.v1i2.557>

Norris, G., Brookes, A., & Dowell, D. (2019). The psychology of internet fraud victimisation: A systematic review. *Journal of Police and Criminal Psychology*, 1–7. <https://doi.org/10.1007/s11896-019-09334-5>

Okeke, C., & Nsirim, O. (2024). Fundamentals of internet and virtual library. In C. O. Udofot, H. I. Wiche, O. Nsirim, B. D. Oladokun, & S. O. Akor (Eds.), *Digital technologies and library management in higher institutions of learning in Nigeria: A Festschrift in honour of Prof. Philip Akor*. Chadwich.

Omidian, F., & Seifi-Maleki, A. M. M. (2013). Information-seeking behaviour on Internet: A comparison between arts and science undergraduate students in Iran. *Turkish Online Journal of Distance Education (TOJDE)*, 14(4), 164–175.

Vohs, K. D., Mead, N. L., & Goode, M. R. (2006). The psychological consequences of money. *Science*, 314(5802), 1154–1156.

Wiche, I. H., Nsirim, O., & Oladokun, B. D. (2024). Cybrary: Navigating the dynamics of library services in virtual environment. Chadick.

Wilson, T. D. (2000). Human information behavior. *Informing Science*, 3(2), 49–55. <https://doi.org/10.28945/576>