THE COLLOQUIUM -A Multi disciplinary Thematc Policy Journal
www.ccsonlinejournals.com
Volume 10 , Number 1 , 2022 Pages 129 – 139
CC-BY-NC-SA 4.0 International Print ISSN : 2971-6624 eISSN: 2971-6632

INTERNET AND COMMUNICATION TECHNOLOGY, A SPACE FOR INTERNET FRAUD: CYBER SECURITY VIA COMPUTER USAGE IN EDUCATIONAL SYSTEM

OLOWU, ThankGod C., OBOT, O. Ph.D & USIP, P. Ph.D
Department of Computer Science,
Faculty of Science,
University of Uyo, Akwa Ibom State, Nigeria
Corresponding Email : olowuthankgod4@gmail.com

Abstract
Today's society is a technological driven and Information Communication and Technology ICT dependent enhanced by educational learning. Although, the internet offers wide range of opportunities for the users to communicate with ease, socialize, achieve, improved job performance and maintain close relationship with others across the globe but there are also risks on other hand. Internet fraud, one of the evils of our time, is becoming a big threat to the society and individuals whose daily activities depend on the use of the computer technology. This paper highlights some of these ICT tools used via computer, examined the fears regarding cyber security threat, highlighted types and nature of threats, stated some causes of internet fraud and the effects of internet fraud. The exponential increase of this crime in the society has become a strong issue and the cyberspace becoming unsafe which cyber fraudsters use the ICT to monitor gas and chemical plants on a safe ground to them for the sales of petroleum products on illegal marketing of the products known as bunkery. This paper provides information that will help the computer and cyber users to be security conscience and as well as to understand different methods internet fraudsters adopt their strategies. Recommendations proffered includes keeping sensitive information about transactions safe, to always ignore e-mail requiring sensitive information, the use of strong password and administrators to be cyber security conscious amongst others.

Keywords: *Big data, cyber security, Educational system,ICT, Internet fraud, Internet of things (IoTs)*

Introduction
Technology today is pervasive. It has permeated virtually all spheres of human endeavour. This has given birth to such buzz words as information age, information superhighway, internet, global village, etc. Recently, however, this has been replaced by such expressions as Internet of Things (IOTs), Big Data, Cyberspace, Cloud Computing, Cyber Security, Data Privacy. Internet is an international computer network that connect all internet computer users that allows individuals access to sending, receiving and storing electronic information over public network. Internet is a conglomeration of two or more web-enabled technology though separated by physical distance but connected together (Aderounmu, 2017) and with profound effects on almost every aspect of human lives. James et al., (2012) assert that the attributes of the Internet – interactivity, global reach, speed, networking facilities, storage capacity - have endeared it to billions of people around the world. Sahara Reporters (2019) reports that as at March, 2019 over 115 million internet users exist in the country, with over 64 million of them accessing broadband services on 3G and 4G networks. Nigeria is the second country in the world that spends most time on the internet

Cite this article as
Olowu, T. C., Obot, O., &Usip, P. (2022). Internet and Communication Technology , a space for internet fraud: Cyber security via computer usage in Educational system. ***THE COLLOQUIUM*****, 10(1), 129-139**.

THE COLLOQUIUM -A Multi disciplinary Thematc Policy Journal
www.ccsonlinejournals.com
Volume 10 , Number 1 , 2022 Pages 129 – 139
CC-BY-NC-SA 4.0 International Print ISSN : 2971-6624 eISSN: 2971-6632

and social media. Internet users in the country navigate the world with computing devices such as mobile phones, tablets and personal computers. All these are powered on the platform of Information and Communication Technology (ICT). This is as well acquired through education system. ICT in education improves engagement and knowledge retention. When ICT is integrated into learning higher institutions, students become more interesting and engaged in using the internet facilities for so many things which could be beneficial to them. This is because technology provides different opportunities to make it more viable and employable in the labour market while to the kids in primary education the learning of ICT is fun and enjoyable to them. The functionalities and conveniences provided by these ICT facilities are seen and felt as we use our laptops or desktop computers, at home, in the cars we drive, the phones we carry about, planes we fly, banks that keep our hard-earned cash, the hospitals that attend to our health care needs, hotel we lodge and some other places we go.

Most of these facilities are networked machines sharing information resources, as the case may be. Threats to our security abound. As stated by one Clive James in Wong (2016), 'it is only when they go wrong that machines reminds you how powerful they are'. This review work is intended as a cyber security conscience, aimed at creating awareness of critical security issues because we are all involved. Wong (2016) aptly put it this way 'protecting that upon which we depend should be front of mind for government, business and industry, academia and every individual with a smart phone in their pocket.' ICT security experts revealed and also warned that the computers controlling machinery in oil in the petroleum industry for infrastructures are vulnerable to attacks by cyber hackers and that more work is needed to prevent control of critical equipment falling into the wrong hands of cyber criminals (Eric, 2019). We need to be very concerned to avert this. The reason for a concern is not far-fetched. Cyber Security Alliance (2012) admits that security and privacy issues are magnified by velocity, volume and variety of big data. Redmiles et al., (2017) opined that the behaviour of the less informed user can influence security and privacy outcomes for everyone else. Based on this, the researcher showed concern to inform the public and education sector on internet evil trend and to be security cautioned. Create or develop a monitory security system that will always avert fraudulent operations.

Conceptual clarification

ICT is a short fall to internet and communication technology and is comprehensible with cyber and internet computer networking that linked other devices for access and sharing of information. A general view of technology is that they are man-made devices of any sort produced to make work easy for humans. Thus, emerging technologies are innovations that assist humans in various ways. The emphasis in this article is the technologies that have to do with data handling and processing. Another relevant concept here is big data. According to Cloud Security Alliance (2012), big data refers to the massive amounts of digital information companies and governments collect about us and our surroundings'. It further reveals that daily, '2.5 quintillion bytes of data – so much that 90% of the data in the world today have been created in the last two years alone". Staggering indeed! ACS Cyber Security Handbook (2016) defines the Internet of Things (IoT):

> "*As encompassing the many and varied devices currently in the market, that will connect to and stay connected to the internet 24/7. Typically this includes products like webcams, smart TVs, and even the much touted internet-connected fridges. But IoT actually encompasses a broad range of products most of which you will not actually see – electronics, sensors, actuators and software soon to be built into everything from your car to your home; technology to unlock your door and*

Cite this article as
Olowu, T. C., Obot, O., &Usip, P. (2022). Internet and Communication Technology , a space for internet fraud: Cyber security via computer usage in Educational system. ***THE COLLOQUIUM*****, 10(1), 129-139**.

THE COLLOQUIUM -A Multi disciplinary Thematc Policy Journal
www.ccsonlinejournals.com
Volume 10 , Number 1 , 2022 Pages 129 – 139
CC-BY-NC-SA 4.0 International Print ISSN : 2971-6624 eISSN: 2971-6632

turn on the lights when you arrive home; technology to also allow your car to talk to other cars and traffic lights to prevent accidents; technology to let entire cities regulate air-quality, manage energy distribution, and regulate water supply all in real-time from thousands of buildings, each with thousands of sensors, all communicating through a city-wide network."

On their part, Fu et al., (2017) posited regarding the Internet of Things (IoT) that "increasingly we live in a world of connected smart devices. This 'Internet of Things' (IoT) combines devices with sensor capabilities and connectivity to the cloud and allows them to leverage artificial intelligence, machine learning, and big data analytics, sometimes dramatically increasing their capabilities."

Cyber space according to the glossary by Taylor & Francis (2009) "refers to the connections and locations (even virtual) created using computer networks. The term "Internet" has become synonymous with this word." Cyber Security is a term used to refer to the protection of everything that is potentially exposed to the Internet, our computers, smart phones and other devices, our personal information, our privacy and our children (The Cyber security handbook, 2013). A red alert, according to dictionary.com is a word when used in (in military or civilian defense) parlance is the most urgent form of alert, signaling that an enemy attack is believed to be imminent. It is also the signal or alarm sounded for this alert. It is also viewed as a signal or warning that a critical situation is developing or has occurred; the period during which a state of crisis or danger is declared to exist. The Mariam-Websters dictionary adds some details to the definition of this word when it says that red alert is the final stage of alert in which enemy attack appears imminent broadly; a state of alert brought on by impending danger. Some synonymous words for red alert include alert, alertness, attentiveness, qui vive, vigilance, watch, watchfulness.

Types and nature of Threats

The Cyber Security Handbook (2013) provides the following as ways our cyber security is threatened:

i.Phishing

This is a means by which criminals trick victims into handing over their personal information such as online passwords, login accounts, social security or bank credit card numbers and information. It might be done by invading your computer with spyware that reads your personal information, or it may be as easy as stalling your wallet. Some may redirect your browser to certain websites, send pop-up ads, and change your computer settings.

ii.Social Engineering

Mitnick (2010) once a notorious computer criminal and now a security consultant, summed up in an August 2011 TIME magazine interview the ways criminals combine plain old psychological trickery with malware-creation skills – a combination referred to as social engineering. He said a hacker may learn your likes and dislikes from your posts on Facebook. "If I know you love Angry Birds (a popular smartphone game), maybe I would send you an email purporting to be from Angry Birds with a new pro version. Once you download it, I would have complete access to everything on your phone," Mitnik said. Through social engineering, computer hackers trick victims into handing over sensitive data – or downloading malware – without thinking twice. Social engineering may take the form of calls or emails or instant messages that appear to come from trusted source. You may get fraudulent email that appears to come from your bank, a shopping website,a friend, or even the State government. The message may even contain links to a counterfeit version of the company's website, complete with genuine-looking graphics and corporate logos. You may be asked to click on a link or fraudulent website which asks you to submit your personal data or account information.

Cite this article as

Olowu, T. C., Obot, O., &Usip, P. (2022). Internet and Communication Technology , a space for internet fraud: Cyber security via computer usage in Educational system. ***THE COLLOQUIUM*****, 10(1), 129-139**.

THE COLLOQUIUM -A Multi disciplinary Thematc Policy Journal
www.ccsonlinejournals.com
Volume 10 , Number 1 , 2022 Pages 129 – 139
CC-BY-NC-SA 4.0 International Print ISSN : 2971-6624 eISSN: 2971-6632

iii.Stuxnet Effect

The Stuxnet effect on gas and chemical pants ensure the prospect of sabotaging industrial control system has been on the radar since 2010 when the news broke that Stuxnet, the infamous cyber-weapon thought to have been developed by USA and Israeli software engineers, had brought uranium enrichment to a standstill at a nuclear facility in Iran during a sustained two years attack. Attacks on US industrial targets climbed from 41 in 2010 to 198 in 2011, the year after Stuxnet, according to US Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). Currently, the attack had reached 245 as at 2014.

iv.Confusing, Deceptive or Non-existent Privacy Policies

Computers have the capability to collect a great deal of information about you, and to transmit that information to third parties including advertisers and advertising networks. For instance, your web browser privacy settings are not tamper proof. Devices like iPhone, iPad and Android phone are capable of tracking your online activities and more. They may include a GPS that knows the device current location or a unique device ID number that can never be turned off.

v.Social Networking

Experts indicate that we use social networking sites at our own risk, and at the risk of exposing our personal information to the world. Nothing online is private. Note that it is too easy to share too much information. Indiscriminate public posts could harm your professional reputation, career and educational prospects, or personal relationships. Many social networking sites allow other people to share information about your or 'tag' you in photos or videos that you would prefer to keep private.

vi.Online Predators, Cyberbullies

Our children could be victims of this. For example, a man pleaded guilty in August 2012 to sexually assaulting two teenage girls he stalked through Facebook. The 29-year-old created a profile using a fake name, pretending to be 17. He "friend" the 14-year-old girls, and began sending sexually explicit text messages. One girl met with him in person, the other rejected his advances – but by reading her Facebook status updates he was able to track her whereabouts. Both girls were sexually assaulted. Befriending teenagers with a fake online identity, gradually coercing them with friendly, then flirtatious, then overtly sexual messages. Using a victim's online posts to learn when and where she would be hanging out. These are common ways sexual predators use the Internet.

One of the best-known cases of cyberstalking from the last decade is that of Jonathan Vance, who hid behind the screen name Metascape, according to media reports. He attempted to take over the Facebook, Myspace, and email accounts of more than 200 girls and young women, ages 14 to 26, and terrorized and blackmailed at least 53 of them into sending sexual photos of themselves.

He had several methods for gaining access to his victims' online accounts. In many cases he used information found on social networking sites and other online databases, such as their birth dates and the names of their schools and hometowns. As described on the previous page, he went to the girls' accounts, clicked the "Forgot Password?" button, and used that information to answer the security questions.

On other occasions, he would contact his victims through instant messaging. Pretending to be a friend or relative, he would say he was locked out of his own online account, and ask for the girl's online password to "borrow" her Facebook, Myspace or email account. In all cases, once Vance had access to his victim's online account, he would immediately change the password – taking complete control over the account. He would then threaten to humiliate the girls by posting embarrassing secrets or other information, unless they sent nude photos. In April 2009, Vance was sentenced to 18 years in federal prison. Broke up, leading to extensive and unremitting verbal humiliation and abuse at school is the actions

Cite this article as

Olowu, T. C., Obot, O., &Usip, P. (2022). Internet and Communication Technology , a space for internet fraud: Cyber security via computer usage in Educational system. ***THE COLLOQUIUM*****, 10(1), 129-139**.

THE COLLOQUIUM -A Multi disciplinary Thematc Policy Journal
www.ccsonlinejournals.com
Volume 10 , Number 1 , 2022 Pages 129 – 139
CC-BY-NC-SA 4.0 International Print ISSN : 2971-6624 eISSN: 2971-6632

of criminals. Two years later, she committed suicide. Mailfence Blog Team (2018) provides the following types of cyber security issues.

vii.Fraud: Fraud is an intentional act to deceive through false information, claim or the suppression of the truth (http://www.businessdictionary.com). Merriam-Webster (2019) defines 'fraud' as deceit, trickery, intentional distortion of the truth in order to induce another person or organization to part with something of value or to surrender a legal right; an act of dishonesty, deception for gain. Fraud is committed when the perpetrator intentionally communicates statements known to be false with the purpose of defrauding the victim of property or something of value. Fraud therefore, involves deceiving a person in order to get the victim give up something in value, usually money to the fraudster as a person or a group.

viii.Internet fraud: Brittanica (2019) defines internet fraud as the use of computer as an instrument to further illegal activities, such as committing fraud, stealing of intellectual property and identities. Internet fraud involves the use of networked communication technology to get peoples' information and use those information to cheat (Omodunbi et al., 2016). Any person who uses a computer network with the intent to obtain property or services by false presence internet commits fraud. Internet fraud is an act of robbery using the internet. Internet fraud operates under different disguises and goes by many names - consumer cybercrime, online fraud and swindles, online crime, e-crime.

Fraud has always been around since human history and it's on victims have not changed Johnny et al., (2009) and Kai et al., (2012). However, with innovations in technology, the Internet has opened up doors for new and more complex methods of internet fraud. According to Onwuegbuchulam (2019), as the federal government of Nigeria embarks on various initiatives to increase access to the internet for Nigerians for positive engagement, the government is conscious of dishonest individuals who are bent on using the internet for illegal activities. They deploy sophisticated systems to intrude connected devices to perpetrate their exploitation schemes', thus making the cyberspace unsafe for genuine users.Internet fraud is a borderless and a non-gender dependent phenomenon. Users, with the knowledge and skill, irrespective of gender, in remote locations can access the technology to further internet fraud; fraudsters are able to target a wide range of potential victims throughout the world, thus exposing secretaries, irrespective of place of work, cadre, age, sex, colour as well as other users to online frauds (Udok, 2019).

Causes of Internet Fraud

The following are some of the identified causes of internet fraud in Nigeria.

a. **High rate of unemployment**: This is one of the major causes of fraudulent activities on the internet in Nigeria. Over 20 million youths in the country do not have gainful employment, National Bureau of Statistics (2019). The inability of some of these youths to be positive engaged has increased the rate at which they take part in criminal activities for their survival. As idle mind is the devil's workshop, most of the youths will use their time and knowledge as a platform for their criminal activities in order to improve their livelihood and to make both ends meet.
b. **Urbanization**: Anah et al., (2012) reiterate urbanization as one of the major causes of internet fraud in Nigeria. Urbanization involves massive movement of people from rural settlements to cities, in search of greener pasture. This results into a heavy competition among the growing populace; as many more educated ones find it lucrative to invest in the crime because the business requires less capital to invest.
c. **Gullible Internet users**: Some internet users are too gullible. They rush at almost every juicy offer/advertisement just to make quick money, without properly investigating sources and

Cite this article as
Olowu, T. C., Obot, O., &Usip, P. (2022). Internet and Communication Technology , a space for internet fraud: Cyber security via computer usage in Educational system. ***THE COLLOQUIUM*****, 10(1), 129-139**.

CC-BY-NC-SA 4.0 International Print ISSN : 2971-6624 eISSN: 2971-6632

genuineness of the offer. Such people are fertile land, which many internet fraudsters take advantage of.

d. **Quest for quick Wealth:** This is another cause of cybercrime in Nigeria. Youths of nowadays are in a hurry to acquire wealth, they are not patient, hence they strive daily to level up with their rich counterparts by engaging in cybercrimes (Omodunbi et al., 2016).
e. **Incompetent security on personal computers**: Some personal computers do not have proper or competent security controls; it is prone to criminal activities hence the information on it can be stolen.
f. **Brazen display of wealth: A nation** that still has many people in need, some prominent Nigerians still display their wealth brazenly most of which they are unable to explain the source. This could fuel the compulsion for a short cut to affluence among the youths.

Common types of Internet scams/Fraud

As the internet is constantly evolving with new ideas, services, methods and accessibility to the internet increases, so the online fraudsters are trying to continually, come up with sophisticated techniques to get people part with money or personal data some of such methods include:

1 **Beneficiary of a Will scam:** This commences with the receipt of a letter or email by the organizational secretaries, that the sender is a named beneficiary of a huge sum of amount or an estate from a Will left behind from a deceased descendant and that the large inheritance is currently in a bank account within the country of the sender. The sender of the letter invites the secretary to assist with the transfer of the money through his/her bank account for 20 (or more) per cent of the millions of foreign currency to be transferred, Once the secretary responds, an advanced fee is sought for '**legal fees**' '**bank transfer commission'** and **currency exchange**. As the secretary becomes more embroiled in the fraud and pays out money, it becomes harder to withdraw. The chance of genuinely wealthy individuals thousands of miles away, and without the sender and receiver knowing each other to truthfully need ones help for such a genuine cause, are slim to non-existence. Needless to say, the majority, if not all, of these invitations are bogus and designed to defraud the respondents.

2 **Wi-Fi eavesdropping.** This is Virtual "listening in" on information over an insecure (not encrypted) Wi-Fi network. The way attackers perform this attack is by placing themselves in the middle (known as MITM attacks) of communications between different parties. The goal is to listen in on the communication in order to steal sensitive information or just to monitor the conversations. Protecting your device and exercising caution will help in protecting your device.

3 **Phoney Charity Fund Fraud**. Charity foundations (Trust or Public) are non-profit making organizations, which help in the process of relieving poverty, supporting disaster (flooding, earthquake etc) relief, and assisting with community projects. Disasters happen daily and people are genuinely in dire need of financial/material assistance. The perpetrators do take advantage of such tragic situation to set up fake websites and rake in donations from unsuspecting internet users. In order to gain the donor's confidence and trust, these fake social pages are backed up with pictures displaying various unpalatable situations of the victims. At times, the fraudsters may pose

Cite this article as
Olowu, T. C., Obot, O., &Usip, P. (2022). Internet and Communication Technology , a space for internet fraud: Cyber security via computer usage in Educational system. ***THE COLLOQUIUM*****, 10(1), 129-139**.

THE COLLOQUIUM -A Multi disciplinary Thematc Policy Journal
www.ccsonlinejournals.com
Volume 10 , Number 1 , 2022 Pages 129 – 139
CC-BY-NC-SA 4.0 International Print ISSN : 2971-6624 eISSN: 2971-6632

as true representatives of a popular charitable organization dedicated to meaningful cause and use high pressure methods (phone calls, regular mails, pictures showing pathetic situations etc) to convince donors to make hefty donations. Truthfully, when some of us hear of a tragic event that hits humanity, we give our supports with an open heart. Nevertheless, such donations never reach the intended good cause.

Fig 1. Phishing message

4 **False phone calls/SMS alerts**: The users of these gadgets can receive phone calls or message alerts purportedly from a relevant government agency (Tax authority, Immigration Office, Pension Commission etc) on the need to update certain personal or organizational records such as international passport, bank verification number, mobile phone number, account access codes, passwords etc. Mostly, the phone users are potential victims which urged them to urgently supply the information to the caller to enable him update the records at his disposal so as not to put the organization where he/she works at disadvantaged position. Such requests, calls or messages are often fake, scam and are surreptitiously used by the sender to drain the victim's accounts.

5.Identify theft: This concept involves the creation of a fake webpage in the name of a bank or similar viable organizations linking forms requesting users to fill-in, their basic information including unique details like Personal Identification Number (PIN), Bank Verification Number (BVN). This is a fastest-growing financial crime. It occurs when a thief assumes the victim's identity in order to apply for credit cards, loans or other benefits, in the victim's name, or uses this information to access your existing accounts. The thief will accumulate massive debt or deplete your current assets and then move on to another stolen identity. The main objective is to retrieve information of accounts of the user; gain access to personal vital information and use it for their own benefits. This could range from stealing online banking details login and password to getting access to ATM and using such to make a lot of illicit money.

6.Phoney Advertisements: The internet is populated with phoney advertisements stating things like '*you have won the lottery, prize promotion or you have been awarded scholarship to study in an overseas country*.' These advertisements state irresistible offers and the targets are advised to **'click here to claim your reward.**' and from one link to another, until asked to supply sensitive details that will lead to loss of money and other valuables. These scams try to trick the people into giving money upfront or supplying

Cite this article as
Olowu, T. C., Obot, O., &Usip, P. (2022). Internet and Communication Technology , a space for internet fraud: Cyber security via computer usage in Educational system. ***THE COLLOQUIUM*****, 10(1), 129-139**.

CC-BY-NC-SA 4.0 International Print ISSN : 2971-6624 eISSN: 2971-6632
personal bank information to receive a prize from a competition that the person never entered. It is more likely to be fraudulent.

7.Black market and counterfeit goods: E-business has become very apparent in the world today. E-business involves the conduct of business on the internet, servicing customers and collaborating with business partners. Computer operators as intensive users of internet do come across and engage in e-business regularly though various e-commerce websites. However, the purchase of an item before actually seeing it has created ways for fraudsters to make money. It is not out of place for the secretary/customers to only find out, after necessary payments, that the seller fails to deliver the item, or that the secretary has bought counterfeit products.

8.Get rich quick scheme: There are all sorts of fake moneymaking opportunities on the internet. Pyramid and Ponzi Schemes fall into this category. The schemes usually lure the unsuspecting investing public to invest as low as ₦1,000 and get as much as eight times the value of the investment as profit or dividend within a limited space of time. Instead of investing the funds of victims, the scheme pays the initial investors using the funds of subsequent investors. Most often, such schemes do fall apart when new investors are insufficient to pay the old investors, or the government uncovers the fraud and steps in and in the end, the perpetrator disappears with the invested money. From any or all of this, computer users are advised by Udok (2019) to 'run as far as away and as fast as possible to avoid burning their fingers.'

9.Social networking sites such as Facebook, Twitter, LinkedIn and Instagram serve as a fertile ground of other types of tricks. Users create fake semi-public profiles and can directly communicate with friends/family and or family members of the original owners without restriction. The fake users go as far as sending messages from the authorised page to friends and family members requesting for money, call cards or any other kind of assistance on behalf of the original owner of the platform for non-existing problem(s) (Michael et al., 2014).

10.Others include fake overseas jobs and employment opportunities, dating, romance and marriage, magazine subscriptions work-at-home, donated equipment for clearance at the ports etc.

Effect of Internet Fraud

According to Anah et al., (2012) & Okeshola et al., (2013), internet fraud is a problem that has become very widespread and come in diverse means, with no limit to the computer users mostly the secretaries that works in big organizations that fall victims. The potential consequence of internet fraud can be damaging and life threatening to the users of these technological gadgets. It can cause considerable distress to the people and can even culminate into serious and enormous financial problems. It can have emotional impacts, health challenges, permanent disability and other lingering effects directly or indirectly on the victims. It can also result into premature death of the person.

At the national level, Olivia (2018) reports that Nigeria is a renowned hotspot for internet fraud as hardly a day will pass without a sort of report. Additionally, Internet fraud is a worldwide problem that is costing countries billions of dollars Anah et al., (2012). According to Ewepu, (2016), Nigeria loses ₦127bn annually to cybercrimes. Through the crime, the international reputation of the nation suffers as well as the nation's national economy, financial, security and health threatened.

Conclusion

ICT and Cyber is an inter-linking network to access other individual information. Is a wonderful technology, making safe ground activities to provides comforts in accessing information for the

Cite this article as

Olowu, T. C., Obot, O., &Usip, P. (2022). Internet and Communication Technology , a space for internet fraud: Cyber security via computer usage in Educational system. ***THE COLLOQUIUM*****, 10(1), 129-139**.

CC-BY-NC-SA 4.0 International Print ISSN : 2971-6624 eISSN: 2971-6632

individuals. However, we must tread on the side of caution as we utilize them. Because they could easily be blades with double edges. Naivety in the use of such devices should never be an option for conscienceless or to relax. Globalization offers unimaginable opportunities for all computer and internet users in terms of access for information, transactions and choice of services. Yet, along benefits are many risks. With the innovations in technology and methods of internet frauds being enhanced by fraudsters, e-fraud are now carried out with greater efficiency and effectiveness and do have potentially greater impact on the individuals and the society. Computer users are potential victims of internet fraud because of their continuous dependence on internet both at workplace and private home, hence advised the computer experts on how to stay safe from becoming victims of the online scammers.

Recommendations

In view of the prevailing situation regarding internet fraud and for individuals not to fall victims, the following simple rules are recommended to be observed by the computer users:

- Don't be gullible; run as far away as possible from the desire to get rich quick syndrome to avoid burning your fingers
- Nigerian security agents should be trained on cyber security threats and how to handle such issues. They should also educate the community about such possible cyber issues
- Avoid pirated software, they could accommodate malware (viruses, Trojans, worms) that get onto the computer and steal information without the knowledge of the user.
- Remain very cautious of the information you receive and share via WhatsApp, email and other social media platforms
- Computer emergency help/hot lines for cyber security matters should be provided and kept functional
- Office Administrators who are at the heart of the organization should be cyber security conscious and bring such issues to the notice off management, because an injury to one is an injury to all.
- Keep sensitive information about yourself - Personal Identification Number (PIN), bank account BVN, ATM card number, place of work, salary/income per annum, email access code away from the social media and internet platforms and never disclose such to unknown persons.
- Always ignore any e-mail requiring your sensitive information or by clicking a link if its security cannot be guaranteed.
- Use strong but different passwords on the various internet platforms that are difficult to guess; employ a combination of characters (upper case and lowercase letters), numbers and symbols – the longer the better - and change them regularly.
- Do not allow unknown person use your cell phones for calls or messages or access to your sensitive information for any transaction.
- Above all, governments should create job opportunities for the teeming unemployed youths. This will go a long way in minimizing the menace.

References

Aderounmu, G. A. (2017). Jobs nowhere, but everywhere: resolving Nigeria's unemployment crisis through information technology, Inaugural lecture series 304 at Obafemi Awolowo university, Ile-Ife, Nigeria

Cite this article as

Olowu, T. C., Obot, O., &Usip, P. (2022). Internet and Communication Technology , a space for internet fraud: Cyber security via computer usage in Educational system. *THE COLLOQUIUM*, 10(1), 129-139.

CC-BY-NC-SA 4.0 International Print ISSN : 2971-6624 eISSN: 2971-6632

Anah, B. H., Funmi D. L., & Julius M. (2012) Cybercrime in Nigeria: Causes, effects and the way out, *ARPN Journal of Science and Technology*, http www.ejournalofscience.org

Baker, T. D. (2012). Digital Confidentiality: A Holistic Security Model for Counselors. Ideas and Research You Can Use. *VISTAS,* I.

Cloud Security Alliance (2012). Top Ten Big Data Security and Privacy Challenges. http//www.cloudsecurityalliance.org.

Burmester, M., Desmedt, Y., Wright, R., & Yasinac, A. (n.d). Security or Privacy, Must We Choose? www. BDWY01.pdf. Adobe Acrobat

Chawki, M. (2009). Nigeria tackles advance free fraud. *Journal of information, law & technology* <http://go.warwick.ac.uk/jilt/2009_1/chawki

Ewepu, G. (2016). Nigeria loses ₦127bn annually to cybercrime — NSA http://www.vanguardngr.com/2016/04/nigeria-losesn127bn-annually-cyber-crime-nsa/

Folorunso, I. O. (2019). Relative effect of peer-tutoring and internet based teaching methods on Polytechnic students' achievement in south west Nigeria, An unpublished PhD thesis submitted to Olabisi Onabanjo University, Ago-Iwoye , Ogun state.

James, C., Natalie, F., & Des, F. (2012). *Misunderstanding the Internet* . Routledge

Johnny, N., Patrick, K., & Ronald, B. (2009) Finding a pot of gold at the end of an internet rainbow: further examination of fraudulent email solicitation, *International journal of cyber criminology, 3 (1)* .https://www.cybercrimejournal.com

Kai, S., Lai, C., & June, W. (2012), An examination of internet fraud occurrences https://www .research gate.net/publication/228460925

Lucian, V., Mathew, W., & David, M. (2003) Defining fraud: issues for organizations from an information systems perspectives 7th Pacific Asia conference on information systems 10-13 July, Adelaide, South Australia

Michael, A., Boniface, A. & Olumide, A. (2014) Mitigating cybercrime and online social networks threats in Nigeria, Proceedings of the world congress on engineering and computer science.

Mitnick, K. (2010). Reprogramming cyber system for reliable data distributions. *Journal of security network and stenography, pp54.*

Cite this article as

Olowu, T. C., Obot, O., &Usip, P. (2022). Internet and Communication Technology , a space for internet fraud: Cyber security via computer usage in Educational system. *THE COLLOQUIUM*, 10(1), 129-139.

CC-BY-NC-SA 4.0 International Print ISSN : 2971-6624 eISSN: 2971-6632

Okeshola, F. B., & Adeta, A.K.(2013). The nature, causes and consequences of cyber crime in tertiary institutions in Zaria-Kaduna state, Nigeria. *American international journal of contemporary research, 3(9), 98-114.*

Olowu, A., & Seri, F. (2012). A study of social network addiction among youths in Nigeria. *Journal of social science and policy review, 4*(1), 98-112.

Onwuegbuchulam, F. (2019). Cybercriminals will continue to make cyberspace unsafe, Osogbo, paper presented at the NCC 109th Telecom Consumer Outreach programme themed Mitigate effects of cybercrimes: The role of telecom consumers held at Osogbo held 4th September

Omodunbi, B. A., Odiase, P. O., Olaniyan, O. M., & Esan, A. O. (2016). Cybercrimes in Nigeria: analysis, detection and prevention. *FUOYE, journal of engineering and technology*, 1 (1), https://www.ajol.info/index,php/fuoyejet

Sahara Reporters (2019, July 17). Nigeria's Internet users hit 115.9 million www.saharareporters.com

Sahara Reporters (2019). Nigeria, second country in the world that spends most time on social media. www.saharareporters.com

Udok, M. (2019). Run away from Loom Ponzi Scheme, Federal Government warns, nation newlead www.nationnewslead.com

Cite this article as

Olowu, T. C., Obot, O., &Usip, P. (2022). Internet and Communication Technology , a space for internet fraud: Cyber security via computer usage in Educational system. ***THE COLLOQUIUM*****, 10(1), 129-139**.