Available online at http://www.journalijdr.com

IJDR

International Journal of
DEVELOPMENT RESEARCH

ISSN: 2230-9926

International Journal of Development Research
Vol. 07, Issue, 06, pp.13287-13291, June, 2017

RESEARCH ARTICLE

ASSESSMENT OF THE TYPES OF CYBER CRIME FACED BY INTERNET USERS IN NORTH-EASTERN NIGERIA

*Fori Emmanuel and Silas Stephen Neji

Ruby Springfield College, P O Box 2205, Maiduguri, Borno State

ARTICLE INFO

Article History:

Received 24th March, 2017
Received in revised form
29th April, 2017
Accepted 15th May, 2017
Published online 30th June, 2017

Key Words:

Cyber-Crimes,
North-Eastern NIGERIA,
Internet Users,
Malicious Software,
Cyber Safety.

ABSTRACT

The main objective of the study was to analyse the types of cyber-crime faced by internet users in north-eastern Nigeria. The research design was cross-sectional in nature. 30 respondents were cyber café operators and 120 were selected from the vast users of the internet. Total sample size was 150. The purposive random sampling technique was used to collect the data. Finding of the study revealed that majority of respondents reported that they were victims of hacking, malware, spamming botnets, phishing, social engineering and cyber stalking. Others are web jacking, password sniffer, and denial of service. Cyber terrorism, online phonography, and piracy were identified as rarely experienced cyber-crimes by both internet users and cyber café operators in north-eastern Nigeria. The best ways to avoid being a victim of cyber-crimes and protecting your sensitive information is by making use of valid and genuine security that uses a unified system of software and hardware to authenticate any information that is sent or accessed over the Internet. Some recommended cyber safety techniques include: use of antivirus software on the system, use of firewall on the system, frequent change of passwords, frequent scanning against spyware, maintaining backup of your important work, installing system software patches, removal of unnecessary software, among other preventive measures.

Citation: Fori Emmanuel and Silas Stephen Neji, 2017. "Assessment of the types of cyber crime faced by internet users in north-eastern Nigeria", *International Journal of Development Research*, 7, (06), 13287-13291.

INTRODUCTION

The Internet is one of the fastest-growing areas of technical infrastructural development. Today, Information and Communication Technologies (ICTs) are omnipresent and the trend towards digitization is growing. The demand for Internet and computer connectivity has led to the integration of computer Technology into products that have usually functioned without it, such as cars, buildings, Electricity supply, transportation infrastructure, military services and logistics – virtually all modern services depend on the use of ICTs. (Shilpa *et al*, 2013). The influence of ICTs on society goes far beyond establishing basic information infrastructure. The availability of ICTs is a foundation for development in the creation, availability and use of network-based services. E-mails have displaced traditional letter, online web representation is nowadays more important for businesses than printed publicity materials; and Internet-based communication and phone services are growing faster than landline communications. The availability of ICTs and new network-based services offer a great number of advantages for the society but not without a number of disadvantages, with cybercrime as one. Cyber-Crime ('computer crime') is any illegal behaviour directed by means of electronic operations that targets the security of computer systems and the data processed by them. In a wider sense, 'computer - related crime' can be any illegal behaviour committed by means of, or in relation to, a computer system or network. The term "cyber-crime" according to Ali and Mehdi, (2010), is the use of a computer and the internet to commit a criminal act such as identity theft, domain theft, Internet auction fraud, blackmail, forgery, embezzlement, online gambling, defamation, pornography, and web sex with minors, violation of intellectual property, cyber terrorism, etc. These are activities primarily directed against computers or network resources, although there may be a variety of secondary outcomes from the attacks. Cyber-crimes have become a real threat today and are quite different from old-school crimes, such as robbing,

Corresponding author: Fori Emmanuel,
Ruby Springfield College, P O Box 2205, Maiduguri, Borno State.

mugging or stealing. Unlike these crimes, cyber-crimes can be committed by an individual and does not require the physical presence of the criminals. The crimes can be committed from a remote location and the criminals need not to worry about the law enforcement agencies in the country where they are committing the crimes. The same systems that made it easier for people to conduct e-commerce and online transactions are now being exploited by cyber criminals.

Forms of cyber crime

Cyber Crime falls broadly under two main categories:

- The disruption or downgrading of computer functionality and network space.
- Illicit intrusions into computer networks

But the United Nations has categorized five offenses as cyber-crime. They include: (i) unauthorized access, (ii) damage to computer data or programs, (iii) sabotage to hinder the functioning of a computer system or network, (iv.) unauthorized interception of data to, from and within a system or network, and (v) computer espionage.

The main forms of cyber-crime are outlined as

Malware -is a general label for malicious software that spreads between computers and interferes with computer operations (Kirwan and Power, 2012). Malware may be destructive, for example, deleting files or causing system ‘crashes’, but may also be used to steal personal data.

Ransomware - is a particularly nasty type of malware that blocks access to a computer or its data and demands money to release it. Example of this is called WannaCry Ransomeware. WannaCry malicious software has recently hit Britain’s National Health Service, some of Spain’s largest companies including Telefónica, as well as computers across Russia, the Ukraine and Taiwan, leading to PCs and data being locked up and held for ransom, (Marsh, Sarah, 2017, The Guardian, 2017, Cox, Joseph, 2017, BBC News, 2017). The WannaCryransom ware attack is an on-going worldwide cyber-attack by the WannaCry ransom ware crypto worm, which targets computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bitcoin cryptocurrency, (technet. microsoft.com, Wikipedia, 2017).

Hacking - the act of gaining unauthorized access to a computer system or network and in some cases making unauthorized use of this access. Hacking is also the act by which other forms of cyber-crime (e.g., fraud, vandalism, etc.) are committed.

Denial of Service or Distributed Denial of Service attack (DoSorDDoS) - relate to the flooding of internet servers with so many request that they are unable to respond quickly enough. This can overload servers causing them to freeze or crash.

Spam - is unsolicited or ‘junk’ email, typically sent in bulk to countless recipients around the world and is often related to pharmaceutical products or pornography. Spam email is also used to send phishing emails or malware and can help to maximise potential returns for criminals.

Botnets - refer to clusters of computers infected by malicious software. They are used to send out spam, phishing emails or other malicious email traffic automatically and repeatedly to specified targets (Alhomoud*et al*., 2013). They are often termed ‘zombies’ as the networks are controlled centrally by a ‘botmaster’ or ‘herder’.

Cyber-terrorism - the effect of acts of hacking designed to cause terror. Like conventional terrorism, `e-terrorism' is classified as such if the result of hacking is to cause violence against persons or property, or at least cause enough harm to generate fear.

Online Pornography - There are laws against possessing or distributing child pornography. Distributing pornography of any form to a minor is illegal. The Internet is merely a new medium for this `old' crime, but how best to regulate this global medium of communication across international boundaries and age groups has sparked a great deal of controversy and debate.

Phishing - is a technique used by strangers to "fish" for information about you, information that you would not normally disclose to a stranger, such as your bank account number, PIN, and other personal identifiers such as your National Insurance number. In other words phishing is the practice of luring users to visit fake Web sites in order to steal passwords, pin numbers and other sensitive information.

Piracy - the act of copying copyrighted material. The personal computer and the Internet both offer new mediums for committing an 'old' crime. Online theft is defined as any type of 'piracy' that involves the use of the Internet to market or distribute creative works protected by copyright.

Social Engineering - is the practice of using personal charm, charisma, deception and trickery in order to elicit sensitive information from the victim.

Cyber-Stalking – is the use of the Internet or other electronic means to harass an individual, a group, or an organization. It may include false accusations, defamation, slander and libel. It may also include monitoring, identity theft, threats, vandalism, solicitation for sex, or gathering information that may be used to threaten or harass. Cyber-stalking messages differ from ordinary spam in that a cyber-stalker targets a specific victim with often threatening messages, while the spammer targets a multitude of recipients with simply annoying messages.

Password sniffer – is a software application that scans and records passwords that are used or broadcasted on a computer or network interface. It listens to all incoming and outgoing network traffic and records any instance of a data packet that contains a password.

Web Jacking – Attack Vector is another phishing technique that can be used in social engineering engagements. Attackers that are using this method are creating a fake website and when the victim opens the link a page appears with the message that the website has moved and they need to click another link.

METHODOLOGY

Objectives

The objective of the study is to assess the types of cyber-crime faced by Internet Users in North-Eastern Nigeria.

Table 1. Distribution of respondents on the basis of the type of cybercrime faced by Internet users in north-eastern Nigeria

		Cyber Café operators (30)		Internet Users (120)	
S/N	Type of Cyber-crime	YES	NO	YES	NO
		Freq. (%)	Freq. (%)	Freq. (%)	Freq. (%)
1	Malware	30 (100%)	0 (0%)	114 (95%)	6 (5%)
2	Ransomware	0 (0%)	30 (100%)	0 (0%)	120 (100%)
3	Hacking	23 (76.7%)	7 (23.3%)	56 (46.7%)	64 (53.3%)
4	Denial of Service (DoS)	19 (63.3%)	11 (36.7%)	84 (70%)	36 (30%)
5	Spamming	30 (100%)	0 (0%)	120 (100%)	0 (0%)
6	Botnets	30 (100%)	0 (0%)	120 (100%)	0 (0%)
7	Cyber-terrorism	8 (26.7%)	22 (73.3%)	16 (13.3%)	104 (86.7%)
8	Online Pornography	3 (10%)	27 (90%)	27 (22.5%)	93 (77.5%)
9	Phishing	27 (90%)	3 (10%)	106 (88.3%)	14 (11.7%)
10	Piracy	2 (6.7%)	28 (93.3%)	19 (15.8%)	101 (84.2%)
11	Social Engineering	29 (96.7%)	1 (3.3%)	116(96.7%)	4 (3.3%)
12	Cyber stalking	28 (93.3%)	2 (6.7%)	110 (91.7%)	10 (8.3%)
13	Money laundering	12 (40%)	18 (60%)	82 (68.3%)	38 (31.7%)
14	Password sniffer	29 (96.7%)	1 (3.3%)	99 (82.5%)	21 (17.5%)
15	Web jacking	30 (100%)	0 (0%)	120 (100%)	0 (0%)
16	Credit card fraud	21 (70%)	9 (30%)	73 (60.8%)	47 (39.2%)

A research design is the specification of methods and procedure for acquiring the information needed. The research design for the present study was cross-sectional research design. Cross-sectional method was used because this method is extensive and can be used to collect data from a large sample at a particular point of time.

Sampling Design

The sample for the present study consisted of 150 respondents (30 cyber café operators and 120 internet users). The purposive random sampling technique was used to select the sample from the selected area.

Methods of Data Collection

As the study is Cross – Sectional in nature, survey method was adopted to collect the information from the target population. A well-structured and pre tested interview schedule was given to the subjects to their response. Interview schedule was used with great care so as to have minimum possible biasness. “English and Hausa” versions of the interview schedule were used.

Data Analysis

For the analysis of data the following steps were followed: (1) Coding: - A coding plan was developed in which code numbers were given to every question and its responses and then tabulated on the coding sheet. (2)Tabulation: - The coded data was transferred from the coding sheet to comprehensive tables to give a clear picture of the findings. (3) Statistical Analysis: - The descriptive statistic applied was frequency and percentage distribution.

RESULTS

The table above indicated that all of the respondents (100%) on both the sides of the cyber café operators and other internet users have received unsolicited or ‘junk’ emails from unknown persons. this is technically known as spamming. 100% of both the cyber café operators and internet users agreed to be affected by web jacking and Botnets. Majority of the internet users (95%) were affected by malware whereas all the cyber café operators (100%) agreed to be affected by malware. 96% of the café operators and 82% of internet users have been victims of password sniffers. While in the case of social engineering, phishing and cyber stalking, majority of the respondents agreed to be victims. The respondents are not in agreement of being victims of cyber terrorism piracy and online phonography. 76.7% of the cyber café operators and 46.7% of internet users agreed to be victims of hacking. Denial of Service (DoS) affected 63.3% of café operators and 70% of internet users. 40% of café operators and 68.3% of internet users were victims of money laundering. And 70% of café operators and 60.8% 0f internet users agreed to be victims of credit card fraud. None of the despondence has ever suffered any attack of Ransom ware by Shadow Brokers.

Conclusion

When any crime is committed over the Internet it is referred to as a cyber-crime. There are many types of cyber-crimes. The growing danger from crimes committed against computers, or against information on computers, is beginning to draw attention worldwide. In most countries around the world, however, existing laws are likely to be unenforceable against such crimes. This lack of legal protection means that users and governments must rely solely on technical measures to protect themselves from those who would steal, deny access to, or destroy valuable information. This study showed that cyber terrorism, online phonography, and piracy are rare cyber-crimes experienced by both internet users and cyber café operators in the north-eastern Nigeria. The most commonly experienced crimes include: hacking, malware, spamming botnets, phishing, social engineering and cyber stalking. Others are web jacking, password sniffer, denial of service among other cyber-crimes.

Recommendations

Cyber-crime and cyber security are issues that can hardly be separated in an interconnected environment. The fact that the 2010 UN General Assembly resolution on cyber security addresses cyber-crime as one major challenge; Cyber security plays an important role in the on-going development of information technology, as well as Internet services. Enhancing cyber security and protecting critical information infrastructure is essential to each nation’s security and economic well-being. Making the Internet safer (protecting Internet users) has become integral to the development of new services as well as government policy.

Deterring cyber-crime is an integral component of a national cyber security and critical information infrastructure protection strategy. There are a variety of different technical countermeasures that can be deployed by cyber café operators to thwart cyber criminals and harden systems against attack. These include:

- Firewalls, network or host based, are considered the first line of defence in securing a computer network by setting Access Control Lists (ACLs) determining which and what services and traffic can pass through the check point.
- Antivirus can be used to prevent propagation of malicious code. Most computer viruses have similar characteristics which allow for signature based detection. Heuristics such as file analysis and file emulation are also used to identify and remove malicious programs. (Glenn and Tony, 2006)
- Microsoft use to issue a patch for affected versions of Windows, ensuring that the vulnerability couldn't be used to spread malware between fully updated versions of its operating system (Surur, 2017). But individuals and organisations are often slow to install such security updates on a wide scale.
- Cryptography techniques can be employed to encrypt information using an algorithm commonly called a cipher to mask information in storage or transit. Tunnelling for example will take a payload protocol such as Internet Protocol (IP) and encapsulate it in an encrypted delivery protocol over a Virtual Private Network (VPN), Secure Sockets Layer (SSL), Transport Layer Security (TLS), Layer 2 Tunnelling Protocol (L2TP), Point-to-Point Tunnelling Protocol (PPTP), or Internet Protocol Security (IPSec) to ensure data security during transmission. (Lammle, 2009).
- Network vulnerability testing performed by technicians or automated programs can be used to test on a full-scale or targeted specifically to devices, systems, and passwords used on a network to assess their degree of secureness.
- Network monitoring tools can be used to detect intrusions or suspicious traffic on both large and small networks.
- Physical deterrents such as locks, card access keys, or biometric devices can be used to prevent criminals from gaining physical access to a machine on a network. Strong password protection both for access to a computer system and the computer's BIOS are also effective countermeasures against cyber-criminals with physical access to a machine. (Doctor Q, *et al*., 2009).
- The use a bootable bastion host that executes a web browser in a known clean and secure operating environment is another deterrent. The host is devoid of any known malware, where data is never stored on the device, and the media cannot be overwritten. The kernel and programs are guaranteed to be clean at each boot. (Weinstein, *et al*., 2009)
- Digital and network forensics deals with discovering and retrieval of information about computer or cyber-crimes to provide court-admissible digital evidence. The problem in network forensics is the huge network traffic that might crash the system if the traffic capture system is left unattended. Kim *et al*. (2004) proposed a fuzzy logic based expert system for network forensics to analyse computer crimes in networked environments and automatically provide digital evidence as cited in (Ali & Mehdi, 2010).

Internet users should take the following precautions

- Social engineers use social media (Twitter, Facebook, Web Sites, etc.) to discover information about the victim (reconnaissance). Be as discreet as possible.
- Do not follow links from e-mail asking you to visit a Web page.
- Be aware of banks, credit cards, utilities, and others asking you to visit their site via unsolicited e-mail link.
- Always make sure that login pages use secure sockets layer (SSL) and that the login pages starts with https://
- Always make sure that the domain name is darker than the rest of the uniform resource locator (URL) when visiting sites. Look for inconsistencies, bad grammar and/or misspelled words on e-mails and web sites as signs of potential fake phishing sites.
- Don't open e-mails with attachments if they are out of context (i.e. iloveponies.pdf from your boss or businessmeeting.pdf from a relative)
- Beware of generic salutations, suspicious email addresses, alarmist messages, request to verify, update or change account settings. Be aware also of unsolicited requests by e-mail to reset your PIN, ID or password.
- Don't open attachments from unsolicited or unexpected e-mails. And avoid opening ZIP files unless you know who it's from and you are specifically expecting it.
- If you get a call from a bank, credit processor, phone company etc. and they ask for private information, DO NOT divulge the information. Instead, ask for their name and extension and call them on the number listed on their corporate Web site. Unless you can positively identify the identity of the person you called, never give out information to an inbound caller.
- Reduce the amount of information about yourself in Facebook, LinkedIn and other social media sites. That information is useful in social engineering.
- Be careful who you add as a friend or connect to when using social media.
- Over 30,000 Web sites get hacked each day, so be aware that even when surfing known Web sites. Don't download and install Apps from unknown Web sites. And don't download and install unsolicited Apps even from known Web sites.
- If you see pop up while surfing, and it's claiming that you are infected with a virus, press ALT+F4 to close the window or CTRL+ALT+DEL to log off. Do not click on any part of the pop up, not even the X to close the window.
- Social Media and Free Services such as Facebook, Twitter, Gmail and others want as much personal information about you as possible so that they can sell it to advertisers (big data). Hackers want the same information so that they can use social engineering to gain unauthorized access to your valuables.
- Rogues are apps usually undetected since smartphone security is in its infancy and smartphones seldom have antimalware. Don't keep sensitive data on your smartphone.

Acknowledgment

I sincerely appreciate the management of the Cyber cafés visited and individual internet users for making the data available for this study.

REFERENCES

Alhomoud, A., Awan I., Disso, J. P., and Younas, M. 2013. 'Cyber security next generation toolkit against botnets', *Computer,* 46(4), pp 62-66.

Ali P., and Mehdi P. 2010. "Internet security - cyber-crime Paradox" *Journal of American Science,*6(1) pp15-24 "An Introduction to Network Vulnerability Testing" (PDF).*Verisign.Retrieved 29 April 2011.*

BBC News 2017,*"Cyber-attack: Europol says it was unprecedented in scale"*available on online athttp//:www.bbc.com/news/world-europe-39907965. *Retrieved 13 May 2017.*

Cox, J. 2017. *"A Massive Ransomware 'Explosion' Is Hitting Targets All Over the World"*available on online at http//www:motherboard.vice.com/en_us/article/a-massive-ransomware-explosion-is-hitting-targets-all-over-the-world. *Retrieved 12 May 2017.*

Doctor Q., Emmet D. and Toby S. (2009) CompTIA A+. Indianapolis, Indiana: *Wiley Publishing Inc,* pp. 560–563.

Dr Mike, M. and Samantha, D. (2013). Cyber-crime: A review of the evidence Chapter 1:*Cyber-dependent crimes Home Office Research Report 75* October 2013.

Eyerys 2017. *"WannaCry Infecting More Than 230,000 Computers in 99 Countries" available online at http:www.eyerys.com/articles/timeline/wannacry-infecting-more-230000-computers-99-countries.Retrieved 13 May, 2017.*

Firewall http://www.tech-faq.com/firewall *Retrieved on 23rd July, 2015*

Glenn, W. and Tony, N.(2006).MCDST self-paced training kit (exam 70-271): supporting users and troubleshooting a Microsoft Windows XP operating system (2nd ed.). *Redmond, Wash.: Microsoft Press.*

Kim, J., Kim, D., Noh, B., (2004). "A fuzzy logic based expert system as a network forensics", *Proceedings of the 2004 IEEE International Conference on Fuzzy Systems, 2*, pp25-29, pp.879-884.

Kirwan, G. and Power, A. 2012. The Psychology of Cyber Crime.*Hershey*: IGI Global.

Lammle, Todd 2009. CompTIA Network+. *Wiley Publishing, Inc.* pp. 427–434.

Marsh, S. 2017. *"The NHS trusts hit by malware – full list".* availableon online at http//:www.theguardian.com/society/2017/may/12/global-cyber-attack-nhs-trusts-malware. *Retrieved 12 May 2017*

Microsoft 2017. *"Microsoft Security Bulletin MS17-010 – Critical".* availableon online athttp//:www.technet. microsoft.com/en-us/library/security/ms17-010.aspx. *Retrieved 13 May, 2017.*

Shilpa, Y., Tanu, S. and Yashika, A. 2013. "Cyber Crime and Security" *International Journal of Scientific & Engineering Research,* 4(8), August-2013.

Sinrod, E. J., Reilly, W. P. 2000."Cyber-crimes: a practical approach to the application of federal computer crime laws", *Santa Clara Computer & High Technology Law.*

Surur 2017. *"Microsoft release Wannacrypt patch for unsupported Windows XP, Windows 8 and Windows Server 2003"*available on online athttp//:www.mspoweruser.com/Microsoft-release-wannacrypt-patch-unsupported-windows-xp-windows-8-windows-server-2003/. *Retrieved 13 May2017.*

Symantec 2012. Internet Security Threat Report 2011 Trends.Mountain View, *CA: Symantec Corporation.* United Nation General Assembly (2010), Resolution adopted by the General Assembly at its 64th session: *GAOR, 64th session, supplementary No. 49.*

Weinstein, C., *et al*. 2009. Modelling and Detection Techniques for Counter-Terror Social Network Analysis and Intent Recognition. *Proceedings from the Aerospace Conference. Piscataway, NJ: IEEE.* pp. 2-10.

****