INTERNATIONAL JOUNAL OF: SCIENCE RESEARCH AND TECHNOLOGY

TIMBOU-AFRICA ACADEMIC PUBLICATIONS
INTERNATIONAL JOURNAL, AUGUST, 2022 EDITIONS
VOL. 10 NO. 9 ISSN: 2623-7861

CYBER CRIME; THREAT AND PREVENTION

***MA'AMUN MUHAMMED; & **SHAMSUDDEEN SURAJO**

**Department of Computer Science, Federal Polytechnic Kaura Namoda, Zamfara State, Nigeria. **Department of Computer Science, Federal Polytechnic, Daura, Katsina State, Nigeria*

ABSTRACT

Over the years, the alarming growth of the internet and its wide acceptance has led to increase in security threats. In the world to-day, several internet assisted crimes known as cybercrimes are committed daily in various forms such as fraudulent electronic mails, pornography, identity theft, hacking, cyber harassment, spamming, Automated Teller Machine spoofing, piracy and phishing.

INTRODUCTION

Today an increasing number of companies are connecting to the Internet to support sales activities or to provide their employees and customers with faster information and services.

The virtual world has taken over the real one, E-business and E-commerce, which are the new mantras and electronic transactions and dominate the overall business paradigm. In this rapidly evolving e-world that depends on free flowing, information there are some major threat that he digital world security is the major problem to be considered.

Security on Internet is challenging. Security on an Internet is important because information has significant value. Implementing security involves assessing the possible threats to one's network, servers and information. The goal is then to attempt to minimize the threat as much as possible. This developing world of information technology has a negative side effect. It has opened the door to antisocial and criminal behavior.

Cybercrime is a threat against various institutions and people who are connected to the internet either through their computers or mobile technologies. The exponential increase of this crime in the society has become a strong issue that should not be overlooked. The impact of this kind of crime can be felt on the lives, economy and international reputation of a nation. Therefore, this paper focuses on the prominent cybercrimes carried out in the various sector and presents a brief analysis of. In conclusion, detection, threat and prevention techniques are highlighted in order to combat cybercrimes.

Keywords: internet, crime, cybercrime, identity theft, hacking, spamming, ATM, phishing e.t.c.

CYBERCRIMES

Cybercrime

Experts debated on what exactly constitutes computer crime or a computer related crime. Even after several years there is no internationally recognized definition of these terms.

Cybercrime was defined as a type of crime committed by criminals who make use of a computer as a tool and the internet as a connection in order to reach a variety of objectives such as illegal downloading of music files and films, piracy, spam mailing and the likes. Cyber-crime evolves from the wrong application or abuse of inter-net services.

Computer Crime

A global definition of computer crime has not been achieved. Cybercrime has been defined as "any illegal unethical or unauthorized behavior involving automatic processing or transmission of data".

Computer Crime is any crime where –

- Computer is a target.
- Computer is a tool of crime
- Computer is incidental to crime

Low-end mobile phones are often referred to as feature phones, and offer basic telephony. Handsets with more advanced computing ability through the use of

native software applications became known as Smartphone (the device under study).

Reason for Cyber Crime

Following are some of the identified causes of cyber-crime (Hassan, 2012)

i. ***Unemployment*** This is one of the major causes of Cybercrime in world. It is a known fact that over millions of graduates in the world does not have gainful employment. This has automatically increased the rate at which they take part in criminal activities for their survival.

ii. ***Quest for Wealth*** is another cause of cybercrime. Youths of nowadays are very greedy, they are not ready to start small hence they strive to level up with their rich counterparts by engaging in cybercrimes.

iii. ***Lack of strong Cyber Crime*** Laws also encourages the perpetrators to commit more crime knowing that they can always go uncaught. There is need for our government to come up with stronger laws and be able to enforce such laws so that criminals will not go unpunished.

iv. ***Insufficient 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.

Source of Cyber Crime, Threat And Attack

Cybercrime threat and attack may come from hacker, organization, criminal network or disgruntled employees. due to increasingly reliance on technology, here are more kinds of attackers running simple sophisticated script, attempting to compromise information.

The following are the most commonly cited attackers

1. ***Terrorist***: Terrorist seek to destroy, incapacity, or exploit critical infrastructure in order to threaten national security, weaken the economy ,and damage public moral and confidence ,terrorist may use phishing schemes or spyware/malware in order to generate funds or gather sensitive information.
2. ***Nation state or Nation Governments***: Network (cyberspace) has increasingly been part of espionage activities by nation, cybercrime or cyber-attack by nation can have a detrimental impact by disrupting

communication, military activities or other services that citizens take for granted on a day-to-day basic.

3. ***Industrial spies***: Industrial spies use computer network for industrial espionage, they seek to use computer network (cyber space) to illegally and unethically steal business trade secret for a competitor to achieve a competitive advantage, secrete such as formulas, design, manufacturing processes, research and future plans in order to protect or expand their shares of the market e.t.c these can be stolen by competitor through network.
4. ***Criminal group:*** Criminal groups seek to attack system for momentary gain, specifically organized criminal groups use spam, phishing and spyware/malware to commit identity theft, online fraud and computer extortion.
5. ***Hackers:*** Hackers are group of people or individual who break into network for the thrill of challenge, bragging rights in the hacking community, revenge, stalking, monetary gain and political activism, among other reason, hacker who hack for political activism are known as hacktivities.
6. ***Disgruntled Insiders***: Disgruntled Insider for cybercrime and threat can include anything from disgruntled employees with access to confidential information to contractors and poorly trained employees who may take actions that risk information

Types of Cyber Crime

i. ***Hacking:-*** Hacking involves gaining unauthorized access to a computer and altering the system in such a way as to permit continued access, along with changing the configuration, purpose, or operation of the target machine, all without the knowledge or approval of the systems owners.
ii. ***Denial of Service Attack: -*** A Denial of Service ("DoS") attack is a rather primitive technique that overwhelms the resources of the target computer which results in the denial of server access to other computers. There are several different techniques that hackers use to "bring down" a server. As the network administrators learn how to limit the damage of one technique, hackers often create more powerful and more sophisticated techniques that force system administrators to continually react against assaults. In order to understand how to apply the law to

these attacks, a basic understanding of the anatomy of the attacks is necessary This is an act by the criminal,, who floods the bandwidth of the victim's network or fills his e-mail box with spam mail depriving him of the services he is entitled to access or provide.

iii. ***Virus Dissemination*: -** This category of criminal activity involves either direct or search unauthorized access to computer system by introducing new programs known as viruses, worms or logic bombs. The unauthorized modification suppression or erasure of computer data or functions with the Internet to hinder normal functioning of the system is clearly a criminal activity and is commonly referred to as computer sabotage.

iv. ***Credit Card Fraud:*** Intangible assets represented in data format such as money on deposits or hours of work are the most common targets related to fraud.

Modern business is quickly replacing cash with deposits transacted on computer system creating computer fraud. Credit card information as well as personal and financial information on credit card has been frequently targeted by organized criminal crimes. Assets represented in data format often have a considerably higher value than traditionally economic assets resulting in potentially greater economic class.

v. ***Computer Forgery*:** This happens when data is altered which is stored in documents that are in computerized form. Computers however can also be used as instruments for committing forgery. A new generation of fraudulent alteration or duplication emerged when computerized colour laser copies became available.

These copies are capable of high-resolution copying, modification of documents that are even creating false documents without benefit of original. They produce documents with an equality that is indistinguishable from original documents. The widespread of computer networks is the need for people with common and shared interest to communicate with each other. Information can easily be represented and manipulated in electronic form. To meet the needs of sharing and communicating information, the computers need to be connected which is called data communication network.

vi. ***Phishing*:-** Phishing, the mass distribution of "spoofed" e-mail messages, which appear to come from banks, insurance agencies, retailers or credit

card companies and are designed to fool recipients into divulging personal data such as account names, passwords, or credit card numbers.

vii. ***Spoofing*:-** Getting one computer on a network to pretend to have the identity of another computer, usually one with special access Privileges , so as to obtain access to the other computers on the network

viii. ***Cyber Stalking*: -** The Criminal follows the victim by sending emails, entering the chat rooms frequently. In order to harass a woman, her telephone number is given to others as if he wants to befriend her.

ix. ***Threatening:*** The Criminal sends threatening email or comes in contact in chat rooms with Victim.

x. ***Salami Attack:*** In such crime criminal makes insignificant changes in such a manner that such changes would go unnoticed.

Criminal makes such program that deducts small amount like ₦ 0.98 per month from the account of all the customer of the Bank and deposit the same in his account. In this case no account holder will approach the bank for such small amount but criminal gains huge amount.

Cyber Threat

Cyber threat is a malicious act that seeks to damage data, steal data, or disrupt digital life in general, it can also be refer to the possibility of a successful cyberattack that aims to gain unauthorized access, damage, disrupt or steal an information technology asset, computer network, intellectual property or any other form of sensitive data. Cyber threats can come from within an organization by trusted users or from remote locations by unknown parties.

Categories of cyber threat

Threats come in two categories:

i. Passive threats:

This involves monitoring the transmission data of an organization.

Here the goal of the hacker is to obtain information that is being transmitted. Passive threats are difficult to detect because they do not involve alterations of data.

A Passive attack attempts to learn or make use of information from the system but does not affect system resources. Passive Attacks are in the nature of

eavesdropping on or monitoring transmission. The goal of the opponent is to obtain information that is being transmitted. Types of Passive attacks are.

a. Release of message content.

b. traffic analysis.

THE RELEASE OF MESSAGE CONTENT–

Telephonic conversation, an electronic mail message, or a transferred file may contain sensitive or confidential information. We would like to prevent an opponent from learning the contents of these transmission

TRAFFIC ANALYSIS –

Suppose that we had a way of masking (encryption) information, so that the attacker even if captured the message could not extract any information from the message.

The opponent could determine the location and identity of communicating host and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of the communication that was taking place.

The most useful protection against traffic analysis is encryption of SIP traffic. To do this, an attacker would have to access the SIP proxy (or its call log) to determine who made the call.

ii. Active threats

These threats involve some modification of data stream or the creation of a false stream. An Active attack attempts to alter system resources or affect their operations. Active attacks involve some modification of the data stream or the creation of false statements. Types of active attacks are as follows:

a. Modification.

b. Denial of message service.

c. Masquerade.

a. Modification of messages –

t means that some portion of a message is altered or that message is delayed or reordered to produce an unauthorized effect. Modification is an attack on the integrity of the original data. It basically means that unauthorized parties not only gain access to data but also spoof the data by triggering denial-of-service attacks,

TIJSRAT
ISSN: 2623-7861

such as altering transmitted data packets or flooding the network with fake data. Manufacturing is an attack on authentication.

b. Denial of Service –

It prevents the normal use of communication facilities. This attack may have a specific target. For example, an entity may suppress all messages directed to a particular destination. Another form of service denial is the disruption of an entire network either by disabling the network or by overloading it with messages so as to degrade performance.

c. **Masquerade** –

A masquerade attack takes place when one entity pretends to be a different entity. A Masquerade attack involves one of the other forms of active attacks. If an authorization procedure isn't always absolutely protected, it is able to grow to be extraordinarily liable to a masquerade assault. Masquerade assaults may be performed using the stolen passwords and logins, with the aid of using finding gaps in programs, or with the aid of using locating a manner across the authentication process.

TYPES OF CYBER THREAT

There are different types of cyber threat and they may generally be classified in different way they affect the computer

I. Computer virus :- this is a software that can replicate itself and infect a computer without the permission or knowledge of his user, A virus can only spread when I is transmitted by computer user over a network or through removable mass storage media computer virus produce a wide variety of symptom on a computer, some virus delete file, reformat the hard disk or cause other damage. others only replicate themselves and may prevent text, videos, or audio message.

II. COMPUTER WORM:-is a piece of software that can self-replicate, malicious software program, worm is very common like virus. Worm is a standalone program that copies itself repeatedly into memory or disk drive untill no more space left. But unlike a virus, it does not need to attach itself to an existing program or require user intervention to spread. it uses a network to send copies of itself to other computer on the network. Worn damage to network by their replicating behaviour, worn consume bandwidth and can degraded network performance.

III. SPAM:-Spam is messages sent to somebody containing unrelated information during internet activity. The purpose of spam is to advertise certain products or services. These ads are usually inserted by viruses, trojans, or worms. Spam is disseminated via email by displaying links to specific sites or files. At this time spam is also disseminated through chat, social media, and programs that are installed on the gadget. The main purpose of spam is for promotion. However, there is also spam containing propaganda and virus content. Spam is very harmful to organizations that use email facilities primarily for military and state activities. Spam can cause stacks on useless messages. It will be fatal. The operating system will not be able to withstand the amount of spam sent to the system. Spam also often contains malware so that the system will send spam to other computers while connected to the internet

IV. SPYWARE:- Spyware is a program that can record secretly any computer network activity. It can steal PIN, password, bank account and others. The recorded data will be sent to the virus maker. If there is valuable data, it will be sold to other parties who can drop the opponent. Spyware deployment cannot be detected. It comes from programs that are downloaded from the internet that is usually already modified and inserted by spyware programs. It can also be infected from sites containing adult content or gambling. Spyware can degrade and damage the performance of the operating system and application programs installed on the computer.

V. Trojan Horse:- Trojan is a piece of software which is often malicious while appearing to perform a legitimate action. Trojan horse often install ‘backdoor program’ which allow hackers a secret way into a computer system. for example you might download a what you think is a new game ,but when you run it ,it delete files on your computer hard disk drive, or the third time you run the game the program email your saved password to another person, Trojan are also referred to as backdoor application, that is the program open a backdoor to your computer giving access to it to a hacker.

PREVENTION'S

Nobody’s data is completely safe. But everybody’s computers can still be protected against would-be hackers. Here is your defence arsenal.

1. Firewalls:

These are the gatekeepers to a network from the outside. Firewall should be installed at every point where the computer system comes in contact with other networks, including the Internet a separate local area network at customer's site or telephone company switch.

2. Password protection:

At minimum, each item they logon, all PC users should be required to type-in password that only they and network administrator know. PC users should avoid picking words, phrases or numbers that anyone can guess easily, such as birth dates, a child's name or initials. Instead they should use cryptic phrases or numbers that combine uppercase and lowercase.

Letters such as the "The Moon Also Rises". In addition the system should require all users to change passwords every month or so and should lockout prospective users if they fail to enter the correct password three times in a row.

3. Anti- Viruses:

Viruses generally infect local area networks through workstations. So anti-virus software that works only on the server isn't enough to prevent infection. You cannot get a virus or any system-damaging software by reading e-mail.

Viruses and other system-destroying bugs can only exist in files, and e-mail is not a system file.

Viruses cannot exist there. Viruses are almost always specific of the operating system involved.

Meaning, viruses created to infect DOS application can do no damage to MAC systems, and vice versa. The only exception to this is the Microsoft Word "macro virus" which infects documents Instead of the program.

4. Encryption:

Even if intruders manage to break through a firewall, the data on a network can be made safe if it is encrypted. Many software packages and network programs – Microsoft Windows NT, Novel NetWare, and lotus notes among others- offer and – on encryption schemes that encode all the data sent on the network. In addition, companies can buy standalone encryption packages to work with individual applications. Almost every encryption package is.

CONCLUSION

Cybercrime is a menace that should be eradicated or reduced to a very minimal level . Several prominent cybercrimes and causes have been discussed in this

paper. The study conducted across the globe has shows that majority of the crimes conducted are carried out by the youths in our society majorly through phishing. Numerous ways have been proposed to prevent future occurrence of this crime, however much can still be done by government and individuals to reduce it. It is recommended that our government should make the welfare and wellbeing of the citizens of paramount importance so as to lessen the burden of individuals by providing good paying jobs and other basic amenities. This will in no little way make life comfortable for people hence reduce their participation in criminal activities for survival. It is only after this is done that any bill or law against cybercrime can really take effect. Individuals are also enjoined to be smart and adhere to the preventive measures listed above in order not to fall victims. Moreover, since youths are the most involved in this crime, there is need for them to be orientated, educated and empowered for the country to have a greater future.

REFERENCE

MichaelA.,Boniface., A. and Olumide, A. (2014) *Mitigating Cybercrime and Online Social Networks Threats in Nigeria*, Proceedings of the World Congress on Engineering and Computer Science Adu Michael Kz, vol. Vol I WCECS 2014, 22–24.

Ndible N., (2016) *Practical Application of Cyber Crime* Issues Retrieved on May 6, 2016 available at: http://ijma3.org/Admin/Additionals/Cybercrime/N

Imran Khan. (2012)Library Hi Tech NewsISSN: 0741-9058 computer virus problem an solution Retrieved 24/03/2022 from https://www.researchgate.net/publication/241849825_An introduction_to_computer_viruses_problemes_and_solutions Dr. prof milind. Dr mr bhaskar v. patil Retrieved 24/03/2022 from https://www.researchgate.net/publication274468580 computer virus: their problems major attack in real life

www.pcsecurityalert.com/pcsecurityalert-articles/computer-virus-prevention.

https://flnerds.com/blog/how-to-prevent-computer-viruses-10-tips-to-keep-your-pc-safe.

https://support.microsoft.com/en-us/topic/how-to-prevent-and-remove-viruses-and-other-malware-53dc9904-0baf-5150-6e9a-e6a8d6fa0cb5

Shandilya A. (2011) *Online Banking: Security Issues for Online payment*, from www.buzzle.com/articles.

Okeshola F.B. and 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, vol. 3(9), 98-114.

Parthiban L. and Raghavan A. R. (2014), *The effect of cybercrime on a Bank's finances,* International journal of Current Research and Academic Review, vol. Volume-2(2), no. ISSN: 2347-3215, 173–178,

Retrieved Feb. 2014 from www.ijcrar.com

Wada F. and Odulaja G. O. (2014), "*Electronic Banking and Cyber Crime In Nigeria - A Theoretical Policy Perspective on Causation,*" Afr J Comp & ICT, Vol 4(3), no. Issue 2.

A Summary of the Legislation on Cybercrime in Nigeria, Legislative & Government Relations Unit, Public Affairs Deparment,Federal Bureau of Investigation (2016), ATM skimming, Retrieved June 8, 2016available online: https://www.fbi.gov/news/stories/2011/july/atm_071411.

Ewepu G, (2016) *Nigeria loses N127bn annually to cyber-crime — NSA* available at: http://www.vanguardngr.com/2016/04/nigeria-losesn127bn-annually-cyber-crime-nsa/Retrieved Jun. 9, 2016.

Iroegbu, E "Cyber-security: *Nigeria loses over N127bn annually through Cybercrime*," available.

http://www.thisdaylive.com/index.php/2016/04/18/cyber-securitynigeria-loses-over-n127bn-annually-through-cybercrime/ Retrieved

Jun. 9, 2016