International Journal of Education and Social Science Research

ISSN 2581-5148

Vol. 3, No. 02; 2020

AN ANALYSIS OF VARIOUS TYPES OF CYBERCRIME AND WAYS TO PREVENT THEM

Samira Ibrahim[1], Daniel Ikechukwu Nnamani[2], Olumuyiwa Ezekiel Soyele[3]

[1]Texas Southern University, Barbara Jordan- Mickey Leland School of Public Affairs,
3100 Cleburne Street, Houston, Texas 77004. America, PH- +1 346-401-7062
mirakaf@gmail.com

[2]Texas Southern University, Barbara Jordan- Mickey Leland School of Public Affairs,
3100 Cleburne Street, Houston, Texas 77004. America, PH- +1 832-946-1426
dnnamani13@gmail.com

[3]Texas Southern University, Barbara Jordan- Mickey Leland School of Public Affairs,
3100 Cleburne Street, Houston, Texas 77004. America, PH- +1 713-474-0706
ezzykul55@gmail.com

ABSTRACT

Over the recent past, the internet has become one of the most crucial parts of people’s daily lives from work to entertainment. Its rapid growth and wide acceptance comes with a cost on privacy and it has thus led to an escalation of security threats. Today, the world experiences many internet-related delinquencies commonly known as cybercrimes that are committed daily. These cybercrimes take place in a number of practices such as phishing, spamming, fraudulent emails, hacking, Automated Teller Machine (ATM) spoofing, identity theft, and cyberbullying. The exponential rise in these cybercrimes has become a strong issue of concern in the current cyber environment. The effects of this form of delinquency can be felt on the economy, lives, and global reputation of technology. Thus, this paper gives a detailed analysis of the prominent cybercrimes taking place in different sectors and the various techniques adopted for preventing these crimes

KEYWORDS: Crime, Fraud, Cybercrime, perpetrators

INTRODUCTION

Cybercrime has been a global economic pandemic with more than $600 billion being lost annually owed to this crime. In most cases, the ways in which this money is lost is through direct transfers from bank accounts of unsuspecting individuals and others through mitigation approaches by financial institutions. Though cybercrimes are difficult to handle, they can be effectively dealt with indirectly by educating the public and the potential victims on the ways to avoid cyber-attacks. This paper looks at cybercrimes and the measures which can be put in place to address the growing cyber-threats in an effective and efficient manner.

Prevalence of cybercrimes

The more the internet is becoming accessible in all corners of the world, so does the risk landscape of cyber environment. This has led to the cybercrime becoming one of the most radical crime in the world resulting to swindling of money and business spying. According to Ewepu (2016), the prevalence of this crime is rampant amongst young people with this being so due to the following factors:

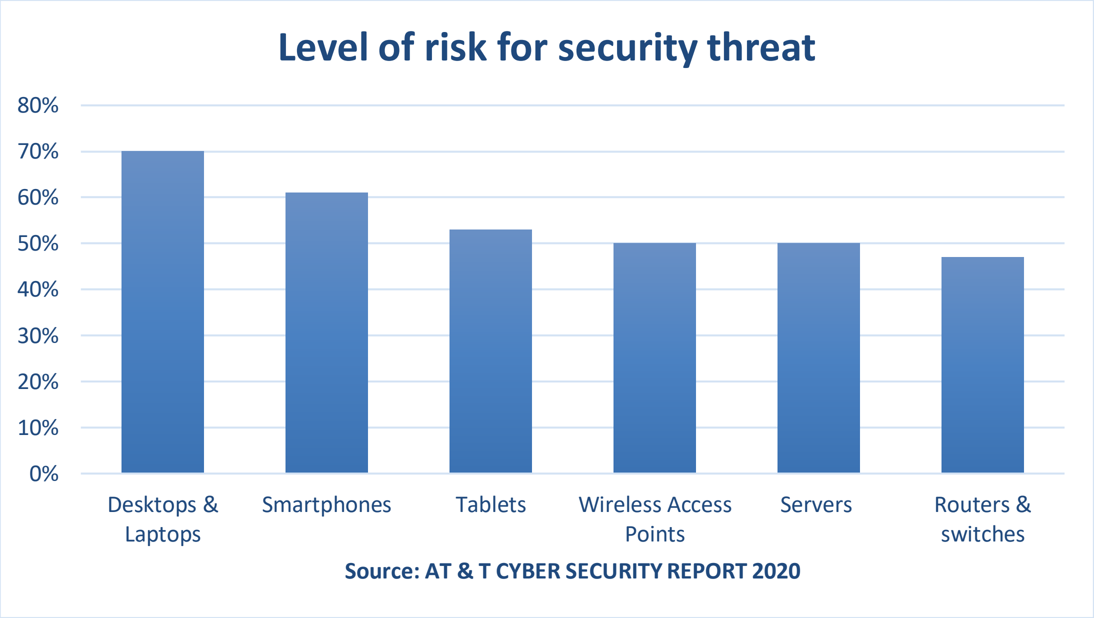
- High unemployment rates: Due to low job opportunities, young people opt to participate in fraud undertakings for their continued existence as they view it as an occupation (Omodunbi et al, 2016).
- Frail cybercrime acts also embolden the criminals to undertake more scam activities deliberate that they will go unpunished as it will not be easy to catch them. Therefore, there is an urgent need to establish stringent laws to discourage criminals from committing such acts.
- A higher incidence of cybercrime is attributed to the great pursuit of wealth attainment. Young people seem to be ambitious, but in actual sense, they are just greedy people who are not prepared to start small (Omodunbi et al, 2016). Thus, they endeavor to equal with the rich counterparts by taking part in cybercrimes.
- The incompetent setting of passwords: with the increase in less concern on password setting amongst many people, fraudsters find loose ends where they extort information and other confidential details that enhance them in their fraudulent activities (Martin, 2016). Having strong security controls is therefore critical in curbing cybercrimes.

With the internet promising more opportunities to businesses, most of them have started to migrate their services online with the banking sector being the main one. Though safety levels in the banking division are becoming robust, the power and maneuvers of the cyber criminals have also intensified with several lucrative attacks having succeeded (Parthiban & Raghavan, 2014). Generally, perpetrators execute deceitful practices with the ultimate objective of retrieving a user's confidential data to rip-off or transfer money to a different bank account devoid of legal consent.

STATISTICAL VIEW

It has been accounted that countries and companies has spent a lot of money when it comes to cybercrime activities. Millions of dollars have been lost through cybercrime activities. The researchers want to use statistical data below to show the mode of penetration of cybercrime in 2020. These information is to make it clear for everyone to be vigilant when using electronic devices that is connected online. Cybercrime is a serious issue; it can hit anyone. That is why (Foster, 2020), emphasis that cybercrime is now becoming a profitable business than the global trade of illegal drugs. Cybercriminals are always believed in a tactics of developing and changing their TTPs (tactics, techniques, and procedure) in other not to be get caught. For the purpose of them making a bigger return from the investment. That is why every individuals or organizations have to stay on top of their games, and tighten all the security of threat and intelligence, and continuously upgrading/ updating their devices with the appropriate software.

Figure 1



Source: AT & T CYBER SECURITY REPORT 2020

Various types of cybercrimes

Biometric Verification Number scam

With the introduction of Biometric Verification Number by many financial institutions, criminals have had the chance to extort money. Fake and unauthorized calls and text messages are sent to different targets demanding personal data including their bank account particulars (Parthiban & Raghavan, 2014). Besides, the creation of phishing sites has increased which allows perpetrators to acquire data for fraud activities on the bank account.

Phishing

Phishing is ubiquitous and has increasingly become one of the rapidly growing cyber-attacks. It involves the theft of identity where fraudsters steal personal data from unsuspecting targets (Omodunbi et al, 2016). In this era, most organizations send regular emails to their members. However, criminals have formulated a way to impersonate ratified organizations and salvage personal data from their customers.

ATM fraud

This form of swindle is carried out through the ATMs and the electronic transaction system. In selected cases, the perpetrator sets up their ATMs where they manage to steal the Pin of the customer or their ATM cards which they later use to withdraw all funds in the client's account. At some point, criminals install hidden cameras to record the ATM pins at distinct places (Martin, 2016).

Sales scam and counterfeit

Presently, the world is faced with the issue of sham sale of goods that are inexistent or those that are replica. The purchase of unseen goods has created a loophole for criminals to exploit; they make cash through the transaction of imitative goods or in some instances, an absent product (Omodunbi et al, 2016). Most people have fallen victims in this particular fraud on popular sites of ecommerce.

Cyber-plagiarism

Information found on the internet has made a successful modification on the approaches in which learners choose to educate themselves. Copy and paste is the commonly used term used to refer to cyber-plagiarism (Omodunbi et al, 2016). Students, particularly the tertiary students undertake this crime without implementing the due penalty.

Illegal e-lotteries

The great desire for many people to get rich quickly especially youngsters are often exploited by cybercriminals who send all sorts of tempting messages of an available lottery bonanza where participants are deceived with numerous items and money ranging from laptops, big cars, and electronics (Martin, 2016). This is one of the most widespread cybercrime.

Advance-fee scam

Most of the impostors obtain finances deceptively from some individuals on the promise of having a contract or on the agreement to getting married (Gnosis, 2009). The criminals usually extort money from the victims by lying that they love the victim and agree to get married. The fraudster will usually convince the victim to send money for travel and other arrangements. Hence, many unsuspecting people become victims of this form of cyber-scam.

Cybercrime Prevention Methods

Government intervention

To effectively handle this cybercrime issue, it is important to establish adequate rules and regulations to address the issue (Michael et al, 2014). The laws ought to be put into words by the federal government and should be followed to the letter by all the involved stakeholders. The law should offer a framework for punishing wrongdoers hence improving the cyberspace safety.

Personal security control

Individuals are expected to maintain strong security controls in their computer systems. Besides, as argued by Lakshmi (2015), individuals are supposed to carefully select the websites they choose to visit. It is advised that one should avoid clicking on untrusted links that appear at the email, Facebook, Twitter, or an advertisement (Michael et al, 2014). Also, it is important to ignore all emails requesting confidential information most especially those requiring financial details. Competency in setting passwords is crucial in ensuring security in a computer system. Individuals should also use rigid passwords/PINs that are hard for anyone to predict. Finally, a person needs to avoid inputting details in an automatically set site as it is always safer to visit the actual site of the seller.

Knowledge- gaining practices

Internet users should make it a habit to constantly update their know-how about the ever-changing nature of information technology. This will not only allow them to be informed, but it will also enable them to gain an understanding of the varying types of cybercrimes and how criminals carry out these deceitful activities. Hence, with this knowledge, individuals can devise ways of protecting themselves from such criminals.

CONCLUSION

Cyber-criminality is a threat and it must be eliminated or minimized to a lower extent for the state to be at peace. Though the crime cannot be eradicated permanently, it can be adequately controlled if the law enforcers administer the laws set to curb cybercrimes. Several cybercrimes such as phishing, ATM fraud, Advance-fee scam, BVM fraud, Academic Plagiarism, and sales fraud have been discussed in the paper. The prevalence of cybercrimes and the factors leading to the high incidence have also been presented. Numerous measures have been recommended to prevent future cybercrimes. However, much is expected from the government as they are the ones responsible for policymaking and enforcement. Individuals are on the other hand advised to being cautious when dealing with cyberspace to prevent them from being victims. However, since the youths have the highest prevalence, the government needs to offer them training, and more empowerment to experience a great future.

REFERENCES

AT &T Cyber Security. (2020, April 17). Retrieved from AT&T Business: https://www.business.att.com/learn/cybersecurity-report-volume-8-5.html

Ewepu G, (2016) cyber-crime — NSA Retrieved from http://www.vanguardngr.com/2016/04/nigeria-losesn127bn-annually-cyber-crime-nsa/

Foster, J. (2020, April 17). 21 Terrifying Cyber Cyber Crime. Retrieved from Data Connectors: https://www.dataconnectors.com/technews/21-terrifying-cyber-crime-statistics/

Gnosis, G. E (2009). Globalization and Transnational Advance Fee Fraud: Journal of Sociology and Anthropology. Vol. 7, No 1

Lakshmi P. and Ishwarya M. (2015), Cyber Crime: Prevention & Detection," International Journal of Advanced Research in Computer and Communication Engineering, vol. Vol. 4(3).

Martin, L (2016). General Introduction to Cybercrime Effects . Retrieved from www.MartinLibrary.com

Omodunbi, B. A., Odiase, P. O., Olaniyan, O. M., & Esan, A. O. (2016). Cybercrimes : Analysis, detection, and prevention. Journal of Engineering and Technology, 1(1), 37-42.

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, Michael., A. 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.