(IJISE) 2019, Vol. No. 10, Jul-Dec **e-ISSN: 2454-6402, p-ISSN: 2454-812X**

A COMPREHENSIVE EXPLORATION OF THE CYBER SECURITY FEATURES AND SAFEGUARDS ALLIED TO THE THREATS AND PROTECTIONS WITHIN THE FRAMEWORK OF THE LAW AND COMPLIANCE SYSTEMS

Ariz Abbas Naqvi

Department of Liberal Arts, Aligarh Muslim University, Aligarh, India

ABSTRACT

With the help of the Internet and digitalization, people have revolutionized their daily lives and activities in the 21st century. Cyberspace is frequently the target of unethical attacks for illegal gains as the digital age advances and becomes increasingly digitalized. It is nearly impossible to locate the attacker due to their cleverness and effectiveness. The sudden increase in cyberattacks has resulted in the development of cyber regulations. This paper provides an in-depth analysis of cybercrime, the fundamental terms used in the field, and related laws and guidelines for increasing cyberspace security.

INTRODUCTION

In this digital age, technology has advanced to the point where it is now an essential part of our daily lives and has begun to have positive and negative effects on everything involved. Having access to everything from visa applications to bank account information to finance documents to tax and bill payments has not only made one's life easier and more comfortable, but it has also led to cyber espionage like data breaches, identity theft, cyberstalking, and privacy violations. Things like these can throw a comfortable life or organization out of whack and jeopardize it. A crime is any illegal act that the state can punish, and when it involves cyberspace and the Internet, it is considered a cybercrime.

A McAfee analysis based on a global poll of more than 800 IT industry CEOs conducted in 2009 [1] indicates that data hacking and related cybercrimes have cost multinational companies one trillion dollars.

Similarly, cybercrime against women and children is rising in India. Chat rooms are the primary cause of this kind of crime. [2]. Compared to previous years, it had reached a significant number [3]. India is seeing an increase in social media-related cybercrimes, with 328 reported in 2017 compared to 155 in 2016 [4].

Undoubtedly, the primary cause of rising cybercrime rates is a need for more awareness and education among individuals. This review paper focuses on the fundamental terminologies of cyber security and cybercrime, as well as the various types of cybercrimes, how to be aware of

(IJISE) 2019, Vol. No. 10, Jul-Dec **e-ISSN: 2454-6402, p-ISSN: 2454-812X**

them and prevent becoming a target, the various types of cybercriminals, and a few case studies to better understand the subject.

CYBER TERMINOLOGY

A. CYBERSPACE

All of the information and space on the Internet that is available together is referred to as cyberspace. Google, Yahoo, and Facebook are frequently used as examples to define cyberspace. According to the White House, cyberspace is a network of numerous computers, workstations, servers, networking devices like routers and switches, and fibre optic connections necessary for communication to continue [5]. Cyberspace is defined by the North Atlantic Treaty Organization (NATO) as a domain that encompasses more than just the Internet; It encompasses individuals and social interaction within these networks in addition to technology, software, and information systems [6]. The Internet, telecommunication networks, computer systems, embedded processor/controller devices, and the interdependent network of information technology infrastructure are all included in the US Défense Department's definition of cyberspace [7].

B. CYBERSECURITY

When we have cyberspace, data, information, systems, and frameworks must be protected from cyber threats. The primary goal of cybersecurity is to keep sensitive data safe and private online by avoiding potential security threats. The practices, strategies, policies, procedures, actions, and technology utilized to safeguard the privacy and property of individuals, businesses, and governments are all included in the broad term "cybersecurity."

C. CYBER LAW

Cyber law refers to the laws and regulations that apply to systems, cyber espionage, and cyberspace. It contains information regarding Internet-related technologies, organizations operating in cyberspace, associated crimes, and the rules and regulations governing their use.

CYBERCRIME

A. CYBERSTALKING

When a person, group, or organization uses cyberspace to stalk and harass another individual or group of committee members and spread negative comments online, this is called cyberstalking. Typically, accusations, uninvited messages, defamation, vandalism, identity theft, and blackmail are all part of cyberstalking. Cyberstalking and harassment typically target women and small business owners.

B. PHISHING

Criminals use forged email exchanges to trick users into giving personal information or installing malware on their computers [8].

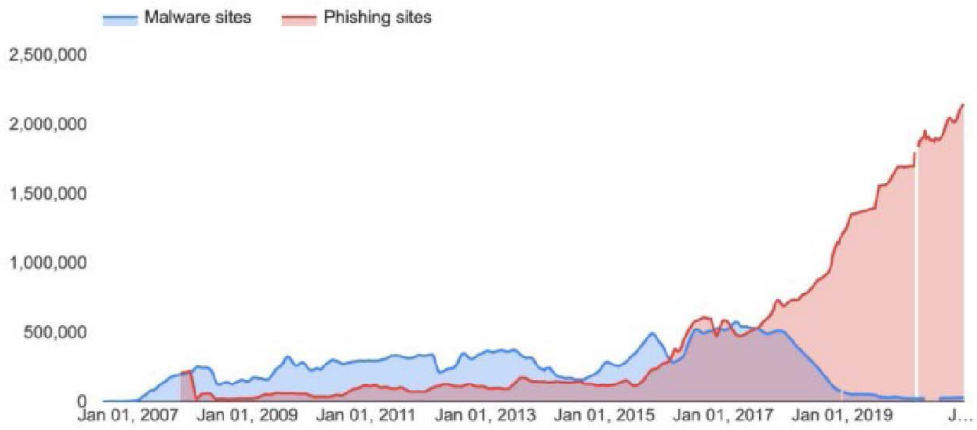
Intruders may delete some information from the victim's computer without noticing it.

The following are the most common methods of phishing:

Link manipulation: Including a malicious link in an email that will send the recipient to a particular website.

DNS CACHE Impairment: DNS (domain name server) traffic is redirected from one IP address to the attacker's IP address.

Google Safe Browsing says that Fig. 1 demonstrates how malware sites have become less popular over time [9].



CYBERCRIMINALS

Age is irrelevant when considering a crime. When considering the various types of cybercriminals, the following can be categorized:

Scripts Most amateur hackers are teenagers or young adults who have learned a few scripts or codes online and attempt to implement them on various platforms to demonstrate their abilities. These actions are usually harmless, but they can sometimes be dangerous, and severe penalties can be taken against those who do them.

Professional Competitors employ certified professional hackers to exploit their rivals and steal sensitive data, such as information about upcoming plans, customers, sponsors, and so on. to benefit themselves personally. These people are hired on a contract basis and perform all of their dirty work.

(IJISE) 2019, Vol. No. 10, Jul-Dec **e-ISSN: 2454-6402, p-ISSN: 2454-812X**

The term "hacktivist" refers to a group of hackers who are typically motivated by political or religious causes.

PREVENTION AND AWARENESS

To learn more about people's and youths' awareness of cybercrime, a questionnaire survey of 200 students was carried out. The following was the conclusion of this investigation into scholars' awareness of cybercrime:

25.1 per cent have a solid understanding of cybercrime.

51.7 per cent - A general understanding of cybercrime

21.7 per cent - Some Knowledge of Cybercrime

1.4 per cent - Do not know about cybercrime.

The result makes it abundantly clear that most people are only somewhat aware of cybercrime. According to a careful analysis of the survey above, most people receive spam calls or messages but have yet to take steps to stop them or alert others. This kind of behaviour is primarily caused by the following:

Lack of awareness of cybercrime or how to deal with it; Inadequate education and training on how to stay safe online; Inadequate awareness of what to do in a cybercrime-related situation

In Fig. 2, the results are analyzed as a graph.

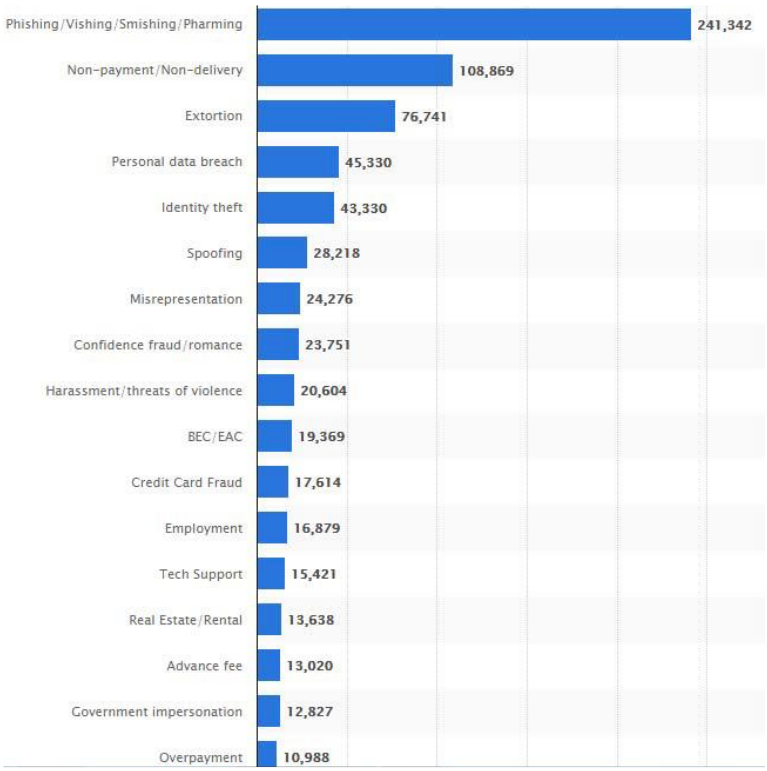


Fig. 2: Survey Analysis of most common cybercrime

Figure 2 demonstrates that phishing is the most frequently reported form of cybercrime.

When carrying out any operation or transaction, you can avoid phishing scams by being cautious and aware of emails and websites.

Never divulge any OTP, CVV, or card information. Continuously recollect that the bank never calls you to recharge your protection and request your subtleties. If you have a problem like this, it's best to go to the branch closest to you. Regular campaigns and education sessions on cyberlaw and cybercrime should be held, especially for young people.

CONCLUSION

This study provides a basic understanding of cybercrime terminology, types of cybercrimes, laws about various cybercrimes, types of hackers, and cyber safety practices. The future ahead will increment cybercrimes, with everyone becoming more challenging to follow and perceptible. Therefore, we should feel safe and take the initiative to alert those around us. To combat cyber espionage, the nation should enact more stringent laws or modify the ones already in place. Only common sense and vigilance can assist us in avoiding losses.

REFERENCES

[1] Alex Roney Mathew, Aayad Al Hajj, Khalil Al Ruqeishi, (2010), Cybercrimes, *International Conference on Networking and Information Technology*.

[2] C. E. Notar, S. Padgett, and J. Roden, (2013), Cyberbullying : A Review of the Literature, *Universal Journal of Educational Research*, vol. 1, no. 1, pp. 1–9.

[3] Christof Baron, IUM Number of cybercrimes related to social media across India in 2016 and 2017, *Statista Research Department.*

[4] The White House, (2003), the National Strategy to Secure Cyberspace, *the White House*, Ed. 2003. [Online]. Available: https://www.uscert. gov/sites/default/files/publications/ cyberspace_strategy.pdf.

[5] NATO Cooperative Cyber Defence Centre of Excellence, *National Cyber Security Framework Manual*, 2012.

[6] U.S. DoD, (2014), *Department of Défense Dictionary of Military and Associated Terms, U.S. Department of Defense*.

[7] Hong, J. (2012). The state of phishing attacks. *Communications of the ACM*, 55(1), 74. doi:10.1145/2063176.2063197

[8] https://economictimes.indiatimes.com//tech/ inter net/cryptojackingis- trending-but-for-how-long/article show/63628338.cms?utm_source =contentofinterest&utm_medium=text&utm_campaign=cppst

[9] Ahluwalia, "Over 900 cases of fraud involving cards, net banking registered in Apr-Sep 2018 //economictimes.indiatimes.com/article show/67977230.cms?utm_source=contentofinterest&utm_medium=t ext&utm_campaign=cppst."

[10] E. Abu-shanab, (2015), Security and Fraud Issues of E-banking, *International Journal of Computer Networks and Applications,* Vol. 2, no. 4, pp. 179–187.

[11] R. G. Sarita Sharma, (2017), Comparative Study and Analysis of Unique Identification Number and Social Security Number, *International Journal of Scientific Research in Computer Science and Engineering*, Vol.5, Issue.1, pp.27-30.

[12] Modi, Krishna. (2017). Review on fraud detection methods in credit card transactions. 10.1109/I2C2.2017.8321781.

[13] Yazdanifard, Assoc. Prof. Dr. Rashad & Wan Yusoff, Wan Fadzilah & Behora, Alawa & Sade, Abu. (2011). Electronic banking fraud; The need to enhance security and customer trust in online banking. International Journal in Advances in Information Sciences and Service Sciences. 3. 505-509. 10.4156/aiss.vol3.issue10.61.

[14] https://www.statista.com/statistics/184083/commonly-reported-typesof- cyber-crime/

[15] https://en.wikipedia.org/wiki/Information_Technology_Act,_2000