The Reviewed Study of Various Techniques to Control and Defeat Cybercrime

Mr. Deshani Gaurav*, Mr. Goda Ronak **, Prof.Dr.C.K. Kumbharana***

DOI: 10.29322/IJSRP.12.03.2022.p12305
http://dx.doi.org/10.29322/IJSRP.12.03.2022.p12305

Paper Received Date: 11th February 2022
Paper Acceptance Date: 2nd March 2022
Paper Publication Date: 6th March 2022

* Research Scholar, Department of Computer Science, Saurashtra University, Rajkot, Gujarat, INDIA, Email: deshani05@gmail.com
** Research Scholar, Department of Computer Science, Saurashtra University, Rajkot, Gujarat, INDIA, Email: ronakgoda@gmail.com
*** Head, Department of Computer Science Saurashtra University, Rajkot, Gujarat, INDIA Email:ckkumbharana@yahoo.com

Abstract- Cybercrimes with the likes of cyber extortion, cyber espionage, stealing and selling corporate data, cyber bullying, phishing, impersonation, and unauthorized systems access have been on the rise over the past decades due to increasing computing technology hence hacking tips as well. These cybercrimes result in massive losses and must therefore be controlled. Their control involves password hygiene practices, the use of encryption, VPN and avoiding public WI-FI, backing up data, use of firewalls, education and mass sensitization, and two factors authentication as discussed in this paper.

Index Terms- Cybercrime, firewall, password hygiene, encryption, authentication, two-factor authentication, phishing, cyber espionage, cyber extortion, and biometrics.

I. Introduction

Cybercrime refers to the use or target of computers or computing resources and infrastructures to commit a crime. Ideally, cybercrime refers to criminal activities that are carried out using computing resources as weapons and targets at the same time. Often, cybercrimes are carried out by malicious hackers intending to make money fraudulently. In other cases, cybercriminals have no intentions to advance economically, and their motivation is to damage the computing networks and resources with an example of critical data just to make it lose its integrity and confidence in use. This case of cybercrimes primarily targets attacking others with no direct economic gain, accounting for the fact if competitors implement such attacks, they will have an ideal opportunity to trade in a less competitive market

II. LITERATURE REVIEW

Cybercrime control refers to methods and techniques that can be applied to mitigate and control the likelihood and chances of a cybercriminal to intercept a computing infrastructure without the authority of the system owner. This access is often driven by malice and results in massive losses, hence exercising sound control. Cybercrime control ensures a computing resources owner that his data is safe and has exceptional integrity, hence confidence when using it. Moreover, cybercrime control mitigates losses accrued to cybercrimes that results in financial losses.

III. OBJECITIVE OF THE STUDY

The objective of this study is to detail methods that can be applied to control and prevent cybercrime. Most cybercrimes in the contemporary world where internet evolution has given the computing field a new lookout include identity and email fraud, cyber extortion, cyber espionage, stealing and selling corporate data, cyberbullying, phishing, impersonation, and unauthorized systems access [1] hence the study strives to include control of the above. Cybercrimes may result in loss of sensitive client’s courtesy of bad reputation, damage of investors' image in the market, and direct financial loss hence the undying need to have cybercrime mitigated.

IV. RESEARCH METHODOLOGY

This study was a success courtesy of the successful use of survey research methodology. Ideally, this study involved extensive consultation of experts in digital forensics and computing infrastructure security. The study also collected significant amounts of information from cybercrimes victims as well as consultation of priory written materials on cybercrimes. This method of study assured the collection of information on where the victims went wrong on security measures and at the same time getting a possible solution to control the scenario in the future.

Factors responsible for cybercrimes

Cybercrimes are promoted by negligence in exercising password hygiene, lack of consciousness on significance and importance of practicing ethical hacking, lack knowledge on computer security, poor timing or lack of regular computer software update, lack of backup, easy system access, and failure to use two-factor authentication. On the other hand, malice and quest for unhealthy competition as well as determination to make easy many through selling stolen data or even extracting money directly from the victim's computing resources.

Cybercrime control

It is essential to appreciate that computing technology, as far as software and hardware is concerned, is evolving quite fast, and so the cybercrime. In most cases, the emergence of a new technology generates a new security loophole that cybercriminals take advantage of before a mitigation strategy is developed. Unfortunately, law and policies develop at a slower pace than computing technology; hence computer-related crimes accounting for the fact that most countries formulate rules and policies on how a specific case of a criminal and a victim should be treated or litigated. Since technology advancement is a single person or a small group's innovation, and so cybercrimes, state rules have no solid justification system on cybercrimes, justice in most cases depends on the strength of evidence which is often hard to compile, especially if the individual or the company lacks forensics knowledge [2]. However, it is important to appreciate rules and government policies play an important cybercrime control role when the issue comes to the limelight. How can one litigate a cybercrime successfully without providing reliable offenders' login details, files shared by the criminal, and whom, when the crime was committed, among other critical details?

Password hygiene

The use of a password is a critical mechanism of preventing and controlling cybercrime cases. This method is quite popular even with naive computer users. Unfortunately, there is something wanting to use passwords in the current century to ensure it meets the primary threshold to control cybercrime, which is password hygiene effectively. Exercising password hygiene encompasses a long list of effective password uses that include using a strong password. A strong password refers to a password that has a combination of capital and small letters, symbols, and numbers at a go. Despite a password being strong, it should not be used for more than one site [3]. Moreover, every computer user must strive to ensure they do not leave passwords on screens written in any form or material near the computer. On the same note, the passwords must be maintained confidential and private and also changed regularly to control cybercrimes that may be committed by malicious ex-employees, with an example of those who are fired hence angered. On the same note, when discarding obsolete computing hardware, it is critical to ensure that it is void of data hence passwords [4]. Controlling possibilities of password leakage translates to controlling cybercrimes that could have been committed with primary facilitation by access of passwords; that is, the cybercriminal has no basic cryptography knowledge hence no hacking.

Multi-factor authentication

The use of two-factor authentication also provides effective cybercrime control. This method falls under proficiency in password use. A multi-factor authentication method refers to the use of more than one method to access computing resources or infrastructures [5]. A two-factor method pertains to the use of a combination of a password and a random code sent to the user by any possible communication means or use of biometrics. Biometrics popularly used includes fingerprints, patterns of the eye retina, facial geometric, and voice records. Two factors authentication control cybercrime by controlling the possibility of an unauthenticated person's access to the computing resources being safeguarded even after succeeding to access the passwords by any means since it is nearly impossible to access the passwords and manage to forge human traits used in biometric authentication [6]. Biometrics single-handedly controls cybercrimes with a significant. This is because they are natural and unique such that forging is nearly impossible. This ascertains exceptionally high security of computing infrastructure and resources at hand hence controlling cybercrimes.

Education and training

Other than using passwords to access protected computing resources maliciously, cybercriminals use social engineering knowledge to phish data from vulnerable and unsuspecting computer users or data owners. Cybercrime statistics claim that the highest numbers of cybercrimes are successful due to a lack of primary knowledge on cybercrimes. As such, computer users tend to open links and emails from cybercriminals in the disguise of people they know. A link or a website with keywords such as "allow" and 'I agree' and their sender has not authenticated poses a great risk of losing data to malicious data phishers [7]. To control cybercrimes committed through, computer users in the private and public sphere should be provided with basic computer security knowledge to keep safe from phishing. This implies they will have basic scrutiny knowledge on the authenticity of a link or an email sent to them by unknown

http://dx.doi.org/10.29322/IJSRP.12.03.2022.p12305

users and contains phishing power. When a computer user with phishing knowledge faces a possible security threat, he knows how to handle, reduce, and control cybercrime cases.

Firewalls

Alternatively, computer users may turn to the use of firewalls that will ensure phishing emails and links are blocked before reaching the computer user. Firewalls are programs designed to scrutinize inbox information and files to ensure it does not contain elements that make it suspicious of being designed to disguise the user as an authentic information sender yet intend to acquire data from the user authentically. When the installed firewalls detect that the incoming files have malicious data phishing intentions, it blocks the file or even the user, depending on the user setting [8]. Ideally, this method strives to ensure that computer users do not become phishing victims, hence effectively controlling cybercrimes.

Sensitization and awareness

Education also has a critical role on matter controlling cybercrimes. Cyber bullying, with an example of using social media platforms for body shaming individuals, insulting, spread racial and discriminatory information, has been on the rise in the contemporary world. These cybercrime aspects have the highest rate of occurrence, and it can be proved by analysis of random posts and comments under the post [9]. Society should be educated on the psychological impact of these crimes on the victims since they result in loss of self-esteem, confidence in public, and when it is extreme, it triggers contemplating suicide. When masses are educated on the importance of social harmony and avoidance of posting reckless and malicious posts, they are likely to acknowledge the sense of avoiding it hence controlling this aspect of cybercrime [10]. On the same note, computer experts should be sensitized to ethical hacking to control malicious cybercrimes that are implemented with no solid sense of benefit, with an example of changing interfering with someone's data to alter its integrity for no sensible gain. Providing education on these aspects will control cybercrimes.

Regular software update

Keeping users' software updated is another significant method of controlling cybercrimes. This is in appreciation that cybercriminals exploit flaws of software to commit their malicious crimes. It takes significantly longer to learn all attributes and loopholes of software. This implies that frequent updates of the software will inconvenience cybercriminals since before they acquire significant knowledge on the loopholes that can facilitate the crime, drastic changes are implemented [11]. When this process continues, cybercriminals may end up giving up. Consequently, this reduces cybercrime by eliminating cybercriminals learning of the loopholes in the software in use by exercising its regular update.

Encryption and avoidance of public WI-FI

Cybercriminals either intercept information in transit or in storage. To control cybercrimes that are implemented on data in transit, it is advisable to embrace strong encryption techniques. The use of VPN contributes to commendable data encryption such that if cybercrimes manage to intercept data in transit, they have another uphill task of decrypting the information. Cryptography knowledge is in possession by a few, and it's rarely successful due to the technicality of the encryption. As such, strong encryption technologies and VPN have significant potential for controlling and preventing cybercrimes [12]. To promote effectiveness of this cybercrime prevention and control method, it is a wise precaution to avoid using public WI-FI such as those provided in hotels, airports and bus terminals, library and cafes since it increases risks of interception of data in transit by cybercriminals posing to be ordinary users of the network provided.

Data backup

Unfortunately, despite being cautious on security measures in computing networks, cybercriminals might identify a loophole. When a cybercriminal makes his way on highly sensitive data, the impact is detrimental and may mean everything is vandalized if the computer users don't have a backup system [13]. The impact is best imaginable of considering a case where a state bank loses its entire data to cybercriminals. The company is left with no information with integrity on creditors, debtors, balances, and other data attribute that have been collected over years of operation. In this case, the backup use is meant to control the impact of the cybercrime rather than preventing it. This is in appreciation that interception on private data must translate to a given impact starting with the loss of integrity, confidentiality, or even direct financial loss; hence having a backup is critical.

V. CONCLUSION

In conclusion, if the worst happens and the cybercriminals make their way on your computing resources and perhaps managed to interfere with it, do not rush to turn off your computer like many naïve computer security rushes to. Instead, it is advisable to first disconnect the computer from any network connection, including the internet. This will terminate data streaming hence sharing of files. Turning off network connections should be followed by calling an expert who will conduct a forensics investigation. After determining what was lost, litigation should take the course while extraction of backup and replacement should be on the high gear as well. In such a case, the digital forensics expert will identify the loophole of the attack and recommend how to handle it. All the same, it must be ensured that password and firewall use is proficient, the user has computer security knowledge, the data is encrypted and backed up among the other discussed cybercrime control.

REFERENCES

[1] Yar, M. and Steinmetz, K.F., 2019. *Cybercrime and society*. Sage.

[2] Holt, T. and Bossler, A., 2015. *Cybercrime in progress: Theory and prevention of technology-enabled offenses*. Routledge.

[3] Kandpal, V. and Singh, R.K., 2013. Latest face of cybercrime and its prevention in India. *International Journal of Basic and Applied Sciences*, *2*(4), pp.150-156.

[4] Jana, F.A.A. and Mondal, S.B.K.K., 2012. A survey of Indian Cybercrime and law and its prevention approach. *International Journal of Advanced Computer Technology*, *1*(2), pp.48-55.

[5] Dasgupta, D., Roy, A. and Nag, A., 2017. Multi-factor authentication. In *Advances in User Authentication* (pp. 185-233). Springer, Cham.

[6] Jagadiswary, D. and Saraswady, D., 2016. Biometric authentication using fused multimodal biometric. *Procedia Computer Science*, *85*, pp.109-116.

[7] Dupont, B., 2019. Enhancing the effectiveness of cybercrime prevention through policy monitoring. *Journal of Crime and Justice*, *42*(5), pp.500-515.

[8] Tailor, J.P. and Patel, A.D., 2017. A comprehensive survey: ransomware attacks prevention, monitoring and damage control. *Int. J. Res. Sci. Innov*, *4*(15), pp.116-121.

[9] Avais, M.A., Wassan, A., Narejo, H. and Khan, J., 2014. Awareness regarding cyber victimization among students of University of Sindh, Jamshoro. *International Journal of Asian Social Science*, *4*(5), pp.632-641.

[10] Kamruzzaman, M., Islam, M.A., Islam, M.S., Hossain, M.S. and Hakim, M.A., 2016. Plight of youth perception on cybercrime in South Asia. *American Journal of Information Science and Computer Engineering*, *2*(4), pp.22-28.

[11] Kandpal, V. and Singh, R.K., 2013. Latest face of cybercrime and its prevention in India. *International Journal of Basic and Applied Sciences*, *2*(4), pp.150-156.

[12] Maimon, D., Howell, C.J., Jacques, S. and Perkins, R.C., 2020. Situational awareness and public Wi-Fi users' self-protective behaviors. *Security Journal*, pp.1-21.

[13] Kamat, P. and Gautam, A.S., 2018. Recent trends in the era of cybercrime and the measures to control them. In *Handbook of e-business security* (pp. 243-258). Auerbach Publications.

AUTHORS

First Author – Mr. Deshani Gaurav, M. Phil (C. S), M.V.M. College of Comm., Mgt & I.T. Rajkot deshani05@gmail.com.
Second Author – Mr. Goda Ronak, M. Phil (C. S), Harivandana College. Rajkot ronakgoda@gmail.com
Third Author – Prof.Dr.C.K. Kumbharana, PhD, Department of Computer Science, Saurashtra University ckkumbharana@yahoo.com

Correspondence Author – Mr.Deshani Gaurav Kiritbhai, deshani05@gmail.com, +919825250880

http://dx.doi.org/10.29322/IJSRP.12.03.2022.p12305