A Criminological Study on Trends of Cybercrimes Against Financial Institutions in Sri Lanka

K.G.L. CHAMUDDIKA[1], K.G.N.U. RANAWEERA[2]
[1] Department of Criminology and Criminal Justice, University of Sri Jayewardenepura, Nugegoda, Sri Lanka
chamuddika@gmail.com
[2] Department of Criminology and Criminal Justice, University of Sri Jayewardenepura, Nugegoda, Sri Lanka
ranaweera@sjp.ac.lk

Abstract

Cybercrimes are virtual crimes that evolved according to nature and the intention of the culprit. Numerous cyber-attacks have been led by several anonymous groups to establish the censorship of information. As the technology used for any activity in the banking industry is continuously upgrading with monetary values as well as with information of clients, it is necessary to have a piece of updated knowledge on both cyber-attacks and technology for both clients and employees of the banking industry. Furthermore, it is crucial to study the nature, techniques and impact of cybercrimes as its techniques are continually evolving with technology. Moreover, it would be possible for individuals to assume that their confidential data and transactions are secured with the bank. This study investigated trends of cybercrimes against Sri Lankan financial institutions using seven Licensed Commercial Banks and uncovered its nature, techniques, impact and strategies that were applied by institutions for the protection of its clients.

Index terms: Cybercrimes, Financial Institutions, Trends, Sri Lanka

References

[1]. B. Yucedal, "Victimization in cyberspace: an application of daily routine activity and life expousre theories," August 2010. [Online]. Available: https://etd.ohiolink.edu/apexprod/rws_olink/r/1501/10?p10_etd_subid=54713&clear=10.

[2]. D. S. Wall, "The Internet as a Conduit for Criminal Activity," INFORMATION TECHNOLOGY AND THE CRIMINAL JUSTICE SYSTEM, no. Sage Publication, pp. 77-98, 2015.

[3]. N. Jayasiri and N. Kariyawasam, "Awareness and Usage of Internet Banking Facilities in Sri Lanka.," International Journal of Scientific Research and Innovative Technology, vol. 03, no. 06, p. 173–190, 2016.

[4]. C. Georgiana and G. C. Piciu, "The Role of Information Technology on the Banking Industry," Annals of the "Ovidius" University Economic Sciences Series, vol. 9, no. 1, pp. 1-14, 2011.

[5]. M. Bachmann, "The Risk Propensity and Rationality of Computer Hackers," International Journal of Cyber Criminology, vol. 4, no. 1&2 January - July 2010 / July - December 2010, pp. 643-656, 2010.

[6]. L. J. Stalans and C. M. Donner, "Explaining Why Cybercrime Occurs: Criminological and Psychological Theories," in Cyber Criminology, Gewerbestrasse, Springer International Publishing, 2018, pp. 25-26.

[7]. E. R. Louderback and O. Antonaccio, "Exploring Cognitive Decision-making Processes, Computer-focused Cyber Deviance Involvement and Victimization: The Role of Thoughtfully Reflective Decision-making," Journal of Research in Crime and Delinquency, vol. 54, no. 05, pp. 639-679, 2017.

[8]. B. Henson, "Routine Activities.," in The Palgrave Handbook of International Cybercrime and Cyberdeviance, Gewerbestrasse, Springer, 2020, pp. 470-489.

[9]. C. J. Howell, G. W. Burruss, D. Maimon and S. Sahani, "Website defacement and routine activities: considering the importance of hackers' valuations of potential targets," Journal of Crime and Justice, vol. 42, no. 05, pp. 536-550, 2019.

[10]. D. Odunze, "Cyber Victimization by Hackers: A Criminological Analysis," Public Policy and Administration Research, vol. 08, no. 01, pp. 08-15, 2018.

[11]. J. Hawdon, "Applying differential association theory to online hate groups: a theoretical statement.," Journal of Research on Finnish Society, vol. 05, pp. 39-47, 2012.