

# Cyber Security to Safeguard Cyber Attacks

**Rishabh SHARMA**

The Shri Ram School (Aravali), Gurgaon, Haryana, India  
rishabhsharmafeb2005@gmail.com

## **Abstract**

*A virtual world or an online world is referred to as cyberspace. It is a communication-enabled artificial world created by computers or internet-enabled devices or components. It is a web-based platform that allows users to interact and communicate with one another. Cybercrime is an area of crime that is rapidly expanding around the world. It is defined as an offense committed using computers or internet-enabled devices. Currently, most of the economic, social, and governmental activities and interactions of countries, at all levels, including individuals, non-governmental organizations, and government institutions, are carried out in cyberspace. Recently, many private companies and government organizations worldwide have been facing the problem of cyber-attacks. With the increasing volume and sophistication of cyberattacks on data at both the personal and organizational levels, there is a greater need to safeguard personal information and sensitive business data. This study aims to comprehensively review the standard advances presented in the cyber security field and investigate the challenges and preventive measures for the proposed methods. Different types of new descendant attacks are considered in detail. The paper will discuss how cyber-attacks steal millions of rupees or dollars from digital wallets and how an individual or organization can save them from such attacks.*

**Index terms:** Cyber-attacks, Cyber security, Digital adoption rate, Organizational models, Economic impact, Reputational loss

## **References**

- [1]. Addae J.H., Sun X., Towey D., Radenkovic M., Exploring user behavioral data for adaptive cybersecurity. *User Model User-Adap Inter* 29(3):701–750. <https://doi.org/10.1007/s11257-019-09236-5>.
- [2]. Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). Cyber Security Awareness Campaigns: Why do they fail to change behaviour? 11.
- [3]. Benson, M. L., Tamara D. M. & John E. E. (2009). White-collar crime from an opportunity perspective. In S. S. Simpson & D. Weisburd (Eds.) *The criminology of white-collar crime* (pp. 175–193). Heidelberg: Springer International Publishing.

- [4]. Bishop M. (2005). "Psychological acceptability revisited." In: Cranor and Garfinkel (Eds), Security and Usability, O'Reilly, pp. 1-11 [chapter 1].
- [5]. Boulton, C. (2017, April 19). Humans are (still) the weakest cybersecurity link. <https://www.cio.com/article/3191088/humans-are-still-the-weakest-cybersecurity-link.html>.
- [6]. Brostoff, S. and Sasse. M.A. (2000). "Are Passfaces more usable than passwords? A field trial investigation." In McDonald S et al (Eds): 'People and Computers XIV - Usability or Else', Proceedings of HCI, Sunderland, UK, pp. 405-424, Springer.
- [7]. Carretero-Gomez, S., Vuorikari, R., & Punie, Y. (2017, April 28). DigComp 2.1: The Digital Competence Framework for Citizens with eight proficiency levels and examples of use, <https://ec.europa.eu/jrc/en/publication/eurscientific-and-technical-researchreports/digcomp-21-digital-competenceframework-citizens-eight-proficiency-levelsand-examples-use>.
- [8]. Cranor, L. and Garfinkel, S. (2005) Security and Usability: Designing Secure Systems That People Can Use. O'Reilly Media, Inc.
- [9]. Gregoric, U., 2010. Socialni inženiring v spletnih socialnih omrežjih. Available online: [http://www.fvv.unimb.si/dv2010/zbornik/informacijska\\_varnost/gregoric.pdf](http://www.fvv.unimb.si/dv2010/zbornik/informacijska_varnost/gregoric.pdf).
- [10]. Landauer, T.K., (1988). "Research methods in Human Computer Interaction." In Helander, M. (Ed.), Handbook of Human Computer Interaction, Amsterdam: NorthHolland, pp. 905-928.
- [11]. Murdoch, S., Drimer, S., Anderson, R. and Bond, M. (2010). "Chip and PIN is Broken". 2010 IEEE Symposium on Security and Privacy. doi: 10.1109/SP.2010.33.
- [12]. Maimon D., Louderback E. R., (2019) Cyber-Dependent Crimes: An Interdisciplinary Review. Ann Rev Criminol 2(1):191–216. <https://doi.org/10.1146/annurev-criminol-032317-092057>.
- [13]. On the (In)Security of Mobile Two-Factor Authentication Alexandra Dmitrienko, Christopher Liebchen, Christian Rossow, and Ahmad-Reza Sadeghi.
- [14]. Ruoti, S., Andersen, J., Heidbrink, S., O'Neill, M., Vaziripour, E., Wu, J., ... Seamons, K. (2016). "We'Re on the Same Page": A Usability Study of Secure Email Using Pairs of Novice Users. Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems, 4298–4308. <https://doi.org/10.1145/2858036.2858400>.
- [15]. Schjolberg, S. Lan, T., Xin, Z., Raduege, H., Grigoriev, D., Duggal, P. and (2008). Global Cyber Deterrence, views from China, the US, Russia, India and Norway, New York: The East West Institute.
- [16]. 2014 SCC Online WIPO 506 Beach Body, LLC v. Cornel Ungureanu /Cyberland LLC World Intellectual Property Organization WIPO, Case No. D2014-0361.