Mini Review
Volume 12:10, 2022

Journal of Mass Communication & Journalism

ISSN: 2165-7912 Open Access

A Factor Analysis of AI-Enabled Social Engineering Attacking Risk in Higher Education

Lina Reijmersdal*

Department of Branding & Technology, University of Bremen, Bibliothekstraße, Bremen, Germany

Abstract

Any sort of business association or individual association single word is exceptionally normal that is data. Contingent upon the data and its correspondence medium guarantee the successful of business. Nevertheless, it is absolutely necessary to comprehend AI-enabled social engineering (SE) attacks and its security risk management strategy. Information is exchanged between nations for a variety of reasons under such circumstances. In that case, any organization should think about a social engineering attack that uses artificial intelligence. These kinds of attacks can disrupt any kind of business venture and prevent the operation of the business while allowing the company to concentrate on its core activities. In the field of information security, one type of criminal activity is social engineering. It has been demonstrated to be a highly effective method for a criminal to gain access to an organization. After obtaining an employee's password through social engineering, the sensitive data were spied on.

Keywords: Social engineering • Threat • Vulnerability • Factor examination • Path model

Introduction

However, any organization ought to be aware of the potential dangers posed by social engineering attacks, which are an inherent risk. This allowed for quick identification and resolution. As a result, the purpose of this article is to explain how social engineering attacks on various organizations were made possible by using exploratory factor analysis (EFA) in artificial intelligence. This, as a result, provides information regarding the most pertinent information security risk factor. 110 of the 300 questionnaires distributed for the study in the education sector were returned for this article. This indicates that 36% of people responded. In that case, the findings of the article demonstrate that artificial intelligence's threat and vulnerability factors enabled social engineering attacks. Therefore, these two aspects pose the greatest information security risk to any organization. Information Security Social engineering is one of the most fundamental types of attacks. Start the attack once the malicious individual has access to the intended victim's information. The survey found that 88% of people who clicked on links in emails reported phishing. Whereas financial institutions are the target of the majority of phishing attacks. Estimating the amount of email sent each day is actually difficult. However, it is said that 90% of email contains viruses or spam. Contrary to popular belief, social engineering is a form of art that involves persuading people to divulge private information. The help desk officer, technical support executive, system administrator, and other positions were the most frequent targets of social engineering attacks [1,2].

Description

A malicious person relies on people's lack of awareness of these values or their carelessness with information security. The significant impact that the attacks have on any organization. This is a financial loss because the company or business venture will lose customer trust. As a result of these attacks, the business wants to make a lot of money. It is the meaning of either going to court or closing the business. Attacks using social engineering ultimately result in the disclosure of any kind of personal information. As a result, maintaining the security of information or information assets is essential to the continued existence of many organizations. Vulnerability and threat are the most significant risk factors for the social engineering attacks that are enabled by artificial intelligence. As a result, the company ought to be aware of this risk factor. When the machine will learn social network behavior, according to the literature review. The artificial hacker will perform at a higher level than the average human. The rate at which an artificial hacker distributes phishing messages will be higher than that of a human hacker. Using a rate of 7.75 messages per minute, one of the artificial intelligences, sent phishing emails to 890 recipients. However, such a quantity cannot be spread for normal use. If such a sum is distributed by the AI. There is actually no issue at all if the AI is put to good use by humans [3-5].

However, the issue arises when a malicious individual instructs the AI to gain access to another system without permission. Though friendly designing is a discipline in sociology. This is the widespread influence of government, the media, or private groups on public sentiment and social behavior. This indicates that social and social engineering terms were initially utilized in social science. Where influential individuals attempted to improperly or improperly motivate others. How this term "social engineering" is used in the world of information security is unknown. There are two distinct types of cybercrime. There are two kinds of crimes: white-colored and black-colored. It is expected that criminals of mind will engage in criminal activity when it comes to black-colored crime. In the case of white-color crime, however, there are intriguing details to be found here. Actually, people of their kind commit crimes, though they may not always possess the necessary skills for information security crimes. It is obvious that computer criminals are not typical computer users—in essence, they are extremely knowledgeable computer users [6-9].

Social engineering now results in the similarity. We are aware that the term "social engineering" is used in social science to refer to a highly influential individual. The same may be true in the information security industry. Here, the term "social engineering" refers to people who are technologically very advanced and have a lot of power. They are attempting to destroy or steal something from a company or organization using this evil power. As a result, both information growth and communication should be controlled and managed by the organization. In order to reduce financial losses, they should manage the rapid growth of information security, particularly in the banking sector. As a result, it clearly demonstrates the significance of analyzing the risk factor [10].

***Address for Correspondence:** Lina Reijmersdal, Department of Branding & Technology, University of Bremen, Bibliothekstraße, Bremen, Germany, E-mail: reijmersdal@googlemail.com*

Received: 01 October 2022, Manuscript No. jmcj-22-83592; **Editor assigned:** 03 October 2022, Pre QC No. P-83592; **Reviewed:** 14 October 2022, QC No. Q-83592; **Revised:** 19 October 2022, Manuscript No. R-83592; **Published:** 26 October 2022, DOI: 10.37421/2165-7912.2022.12.489

Conclusion

This paper demonstrates the social engineering-based risk factor using artificial intelligence. That information, as previously stated, is priceless. So, security threats like phishing, spam, intrusion, worms, employee sabotage, and data or information theft for financial gain. It is obvious that the AI was created by malicious individuals solely for financial gain. In point of fact, the malicious individual has no interest in the data of normal people. According to a survey conducted by the Federal Bureau of Investigation (FBI) in 2018, 5066 organizations discovered that computer-related crimes like PC theft, viruses, and spyware are on the rise and would cost U.S. businesses a staggering US 76.5 billion annually (news.cnet.com, 2018). It is obvious that comparable wrongdoing might occur in emerging nations and other under non-industrial nations

References

1. De Vries, Lisette, Sonja Gensler and Peter SH Leeflang. "Effects of traditional advertising and social messages on brand-building metrics and customer acquisition." *J Mark* 81 (2017): 1-15.
2. De Vries, Lisette, Sonja Gensler and Peter SH Leeflang. "Effects of traditional advertising and social messages on brand-building metrics and customer acquisition." *J Mark* 81 (2017): 1-15.
3. Gu, Xian, and P. K. Kannan. "The dark side of mobile app adoption: Examining the impact on customers' multichannel purchase." *J Mark* 58 (2021): 246-264.
4. Hoekstra, Janny C., Peter SH Leeflang and Dick R. Wittink. "The customer concept: The basis for a new marketing paradigm." *J Mark Manag* 4 (1999): 43-76.
5. Jullien, Dominique. "A letter from the outgoing editor-in-chief." *Romanic Rev* 97(2006): 261.
6. Ahmed, Naheed. "Measurement of perceived interpersonal and societal anti-Muslim discrimination in the United States." *Assessment* 28 (2021): 668-681.
7. Banales, Josefina, Adriana Aldana, Katie Richards-Schuster and Constance A. Flanagan et al. "Youth anti-racism action: Contributions of youth perceptions of school racial messages and critical consciousness." *J Commun Psychol* 49 (2021): 3079-3100.
8. Byrd, Christy M. "The complexity of school racial climate: Reliability and validity of a new measure for secondary students." *Br J Educ Psychol* 87 (2017): 700-721.
9. Diemer, Matthew A., Adam M. Voight, Aixa D. Marchand and Josefina Bañales. "Political identification, political ideology, and critical social analysis of inequality among marginalized youth." *Develop Psychol* 55 (2019): 538.
10. Godfrey, Erin B and Justina Kamiel Grayman. "Teaching citizens: The role of open classroom climate in fostering critical consciousness among youth." *J Youth Adolesc* 43 (2014): 1801-1817.

How to cite this article: Reijmersdal, Lina. "A Factor Analysis of AI-Enabled Social Engineering Attacking Risk in Higher Education." J Mass Communicat Journalism 12 (2022): 489.