Article Analysis on Cybersecurity Awareness

Amira Muaket

Old Dominion University

CYSE 201s

Professor Matthew Umphlet

July 16, 2024

Abstract

The article I will be using is “Factors Affecting Cybersecurity Awareness among University Students.” by Mohammed A. Alqahtani. It focuses on the importance of cybersecurity awareness and what factors are affecting the knowledge of security among university students. Factors that were pointed out and studied were “password security, browser security, and social media” as well as the students prior. Mohammed created an online survey for all university students regardless of age and gender and it comprised 15 multiple-choice questions relating to students’ online behavior and their knowledge of cybersecurity. The test was conducted at Imam Abdulrahman Bin Faisal University in Saudi Arabia and was taken by both undergraduate and post-graduate students, receiving 450 responses. Overall, we can examine how this article relates to the social science aspects, principles, and ideologies specifically in education and awareness directed to the public while stressing the importance of cybersecurity implications, policies, methods, and frameworks.

Article Analysis on Cybersecurity Awareness

The topic of this article centers around cybersecurity insights and factors such as password, social media, and browser security, as well, as its influences on cybersecurity awareness in students. Relating this topic to the Principles of Science and its connections to cybersecurity, of the 7 Social Order, by Robert Bierstedt (Relativism, Objectivity, Parsimony, Empiricism, Ethical Neutrality, Skepticism, and Determinism), I believe Parsimony, Empiricism, and Objectivity principles are applied throughout the article, as it assists in emphasizing key social science aspects. Parsimony provides studies and explanations in the most simplistic ways possible, allowing access and knowledge to be available to everyone this article demonstrates a simplistic way of identifying key issues with cybersecurity awareness and college students, such as implementing a survey and gathering results to be displayed. The author also points out the importance of how cybersecurity awareness should be simplified and available "Cybersecurity awareness and training programs might be an element of national security and they should be well-structured to provide people with a basic grasp of cyber security."(Alqahtani, 2022). Next is Empiricism and it is composed of conducting studies that are real to the senses, meaning this principle focuses on evidence-based strategies versus intuition or hypothetical instances. In this article, the author used surveys to conduct his research and provided statistical analyses in the responses by using a software called SPSS (Statistical Package for the Social Sciences) and a statistical tool called ANOVA (Analysis of Variance). Finally, Objectivity refers to research that isn't opinion-based, meaning researchers are there to provide knowledge and address key issues versus opinionated responses on certain subjects. The author addresses key concerns around

cybersecurity awareness, without having any personal biases, as the article is used for knowledge and further the importance and understanding of cybersecurity.

The study's question/hypothesis was what are the main factors contributing to/affecting cybersecurity awareness by addressing the need to implement effective cybersecurity awareness programs while centering the importance and testing of password security, browser security, and social media among the students. The main outcome of this survey and article is to educate and assist students to become more aware and informed of cybersecurity aspects. The materials and methods used in the article were an online survey, using fifteen multiple choice questions and splitting it into three sections: Secortion one covered password-related questions(for example: Is your password more than 12 characters?) and it had 6 questions. Section two asked browser security-related questions(for example: Are you regularly updating your web browser?) and had 4 questions, and Section three asked social media-related questions (for example: Is accepting friend requests or invitations from strangers seem okay?) and had 5 questions. The question choices revolved around five responses which were “Strongly Agree, Agree, Neutral, Disagree, Strongly Disagree”.

The author collected 4 forms of data from 450 participants. The first is demographic data, which collected data based on gender, age, type of degree held, basic computer skills, and the regular use of online purchases. Demographics were needed to gain a basic understanding of the participants in determining the results of each question/section. The second form of data was section one of the question which is password security. It concluded that results were low around this area, since students weren't aware that passwords should be changed periodically, didn't care for the length of the password, and used the same password for all applications. The third form of data was regarding browser security, results concluded that students scored relatively high on

web awareness, specifically in regularly updating the browser, not accepting installing or using extensions from third-party websites, and periodically checking the security and configuration settings of web browsers. Finally, the fourth form of data was about social media usage and the results showed that students also scored high, as they strongly disagreed with sharing personal information/photos online and understanding how to report suspicious behavior. Regarding accepting friend requests from strangers students seemed naturally around that subject. The results concluded that password security, browser security, and social media had a significant influence on the students and opened the discussion of implementing better cybersecurity awareness. Although the students reported high scores regarding browser security and social media usage there was still a huge decline regarding password security, as well as, not everyone was fully aware of these 3 subjects. This test also spread awareness among the participants as they are more aware of the importance of cybersecurity, and beginning to implement practices sustained from cybersecurity methods and frameworks.

The article also displayed various concepts of social sciences regarding cybersecurity such as the connection of social science research methods to cybersecurity, human factors, the importance of cybersecurity culture, and social science in the lens of education. We can examine how research methods of social science can be used and implemented in the scope of cybersecurity, such as what the article displayed. The social science research method consists of producing a question, creating a hypothesis, conducting experiments, and providing variables. We can also see how cybersecurity can conduct different research methods such as archival research, other variations of field studies(Traditional, Cyberspace, and honeypot field studies), and multi-method research. The article took a multi-method approach since it combines cybersecurity from a social science point of view. Also, it used various research methods when

addressing the concern, such as surveys, analysis tools, and ideas and experiments from other distributors.

Next is human factors, this article is based on cybersecurity awareness by using human participants, showing the connection between technical elements and human behavior. Humans are the biggest cybersecurity risk, but also the strongest defenses against cybercrime. “Humans are susceptible to cognitive biases, such as the tendency to prioritize convenience over security or to underestimate risks when they perceive a task as familiar. By recognizing these biases, cybersecurity professionals can tailor their approach to mitigate human error effectively.” (SecurityScorecard, 2024) In this article we can conclude that the biggest factor that many participants failed on is password security, many were unaware or didn't care for passwords, which allowed us to understand user behaviors and errors. Once understanding the errors, researchers and system operators can educate users on the importance of cybersecurity and create awareness programs to help combat these issues.

This article also points out the importance of cybersecurity culture, since it places routine on how to use and protect yourself and others when engaging online. Creating sort of a community, where people can empower each other in awareness and use proper techniques to combat cybercrime. The author points out how cyber security culture in worldwide settings isn't placing importance on cybersecurity, as well as addresses how the cybercrime rate has extremely skyrocketed due to the lack of awareness and negligence of cybersecurity components. “The global trend in cyber security issues is primarily because most personnel do not adequately adhere to the specific security regulations and instructions supplied in the workplace.”(Alqahtani, 2022)

Finally addressing social science in an education discipline, paves the way for designing and implementing various education methods and programs to assist in awareness and knowledge regarding cybersecurity. Education also provides a wide range of different digital literacies and skills that one can apply to day-to-day activities, enhancing security on technical devices such as computers, smartphones, tablets, smart homes, etc. The article displayed a clear indication of how this survey enhanced the knowledge of cybersecurity and provided their question/hypothesis right. "Based on the research conducted, it can be concluded that knowledge of password security, browser security, and social media activities significantly influence cybersecurity awareness in students. Overall, students have realized the importance of cybersecurity awareness."(Alqahtani, 2022)

The article's topic has challenges regarding digital inclusivity, specifically in the lack of awareness and inadequate infrastructure. Concerns regarding lack of awareness and education can stem from various challenges, especially in marginalized communities since they are more prone to phishing attacks, malware, viruses, hacking, etc. due to the lack of cybersecurity awareness. Contributions can enforce cybersecurity ideologies and awareness since education is an effective measure against cybercrime. "Effective policy and regulatory frameworks are essential for safeguarding privacy and cybersecurity. Governments should enact and enforce laws that protect personal data and ensure that digital service providers adhere to stringent security standards."(Digital Frontiers Institute, 2024) Another concern that can be addressed is inadequate infrastructure, low-income areas usually have limited resources and opportunities to have cybersecurity implementations. Contributions can be investments in more community centers and affordable security solutions, "governments and private sector partners can collaborate to develop low-cost cybersecurity tools and services that are easy to deploy and

use.”(Digital Frontiers Institute, 2024). Other contributions can be using encryption and multi-factor authentication as another way to combat cybercrime and enhance cyber security.

Overall, this article highly contributes to society and addresses crucial points that society suffers from. One is negligence and ignorance when it comes to cybersecurity while addressing and understanding various factors that contribute to the issue. The author stresses that even though some may be aware of cybersecurity and can protect themselves, it is not enough, it must be a communal effort from areas and communities to tackle this situation and provide ways to overcome such situations. Personal and national security must address and implement cybersecurity as it will assist in a better cybersecurity culture. Another important point that this article addresses is the advancement of education, by creating various ways to educate audiences from all over the world, regardless of language and certain areas, since anyone can be a victim of a cyberattack/threat. Many can adapt new skills and knowledge to help themselves and communities that suffer from different factors such as marginalized areas and different environmental influences.

References

Alqahtani, M. A. (2022). Factors Affecting Cybersecurity Awareness among University Students. Applied Sciences, 12(5), 2589. https://doi.org/10.3390/app12052589

May. R. (2017). Your Human Firewall – The Answer to the Cyber Security Problem TEDxWoking. In YouTube. https://www.youtube.com/watch?v=BpdcVfq2dB8

Learning Center. (2024, February 16). The Human Factor in Cybersecurity. SecurityScorecard. https://securityscorecard.com/blog/the-human-factor-in-cybersecurity/#:~:text=Humans%20are%20susceptible%20to%20cognitive

Digital Frontiers Institute. (2024, June 13). Cybersecurity and Privacy in an Inclusive Digital Economy: Safeguarding the Vulnerable. Digital Frontiers Institute. https://digitalfrontiersinstitute.org/cybersecurity-and-privacy-in-an-inclusive-digital-economy-safeguarding-the-vulnerable/

Module 4, Module 2, Module 3, Module 9 Canvas PowerPoints