Journal on Technical and Vocational Education (JTVE), Vol 10, No 1 (2025)
eISSN: 0128-0821
http://upikpolimas.edu.my/ojs/

FACTORS INFLUENCING ONLINE SCAM AWARENESS AMONG MALAYSIAN CIVIL SERVANT

Suhaini Mat Daud, Intan Shafina Suid, Hayazi Hanafi
Politeknik Sultan Abdul Halim Mu'adzam Shah[1,3], Politeknik Tuanku Syed Sirajuddin[2]

Abstract: The study of on online scams in Malaysia is still in its infancy, despite the increasing the number of reported cases in the country. Through a comprehensive analysis of key variables which are attitude, knowledge and environment, the study explores their relationships and the implications for scam awareness in the digital landscape. This study primarily aims to investigates the factors influencing online scam awareness in Malaysia among civil servants. A quantitative research method is employed, with data collected through purposive sampling. The collected data is analysed using the statistical analysis of IBM SPSS Statistics version 26. The sample consists of 144 Malaysian civil servants. The researcher distributed the questionnaire to the respondents via a Google Form link. The findings indicate that respondents have a high awareness of online scams. Additionally, the findings reveal that attitude, knowledge and environment correlate with online scam awareness.

Key words: *Online scam, civil servants, purposive sampling, attitude*

1.0 Introduction

The advancement of technology has altered social norms. The Internet is a global network that serves as a communication platform regardless of age or time, whereby mobile device tools and computer networks are required as operational communication aids. The rise of smart gadgets, e-commerce, and social media has led to an increase in the amount of our daily activities, such as payment, banking, and social interactions and payments (Lin et al., 2023). Although using the internet has many benefits, it also has many drawbacks. The rapid expansion of our online routines has opened new opportunities for cybercriminals to engage in various forms of scams, allowing them to carry out traditional scams on an industrial scale at minimal cost, even devising entirely new scam schemes. As a result, many people who were such crimes would not have been intentionally targeted in the past are now at risk of becoming victims daily (Button et al., 2014).

According to Cross and Blackshaw (2014), an online scam occurs when a person interacts with a fraudulent invitation, request, notification, or offer online and experiences a negative impact or money or non-financial loss. The prevalence of these scams in Malaysia is evident in the data reported by the Ministry of Communications and Digital (2022), which recorded 98,607 cases between 2017 and 2021, resulting in total losses of RM3.3 billion. In efforts to combat these activities, the Securities Commission Malaysia (SC) reported taking action in the first quarter of 2023 by blocking 61 websites and 80 social media accounts, and adding 84 entities to its Investor Alert List (The Star, 2023).

Online scamming has become a significant concerned in Malaysia, with a steep increase in fraud cases over the past decade. In 2019, there were 13,703 reported cases resulting losses of RM539 million. This trend continued in 2020, with 17,227 cases causing RM511 million in losses. In 2021, the number of cases rose to 20,701 with losses reaching RM560.8 million. From January to July 2022, there were 12,092 cases, leading to losses of RM414.8 million (Bernama, 26 September 2022). Most recently, from January to October 2024, the total loss due to online scams reached RM1.22 billion (Hidayath Hisham, 2024). Additionally, 181,628 phone numbers, 222,092 bank account numbers, and 1,395 company names have been linked to these scams. Civil servants are particularly vulnerable to online scams due to their perceived financial stability and access to sensitive information. Many individuals have lost significant amounts of money to these scams, costing Malaysia millions of ringgits (Jusoh & Nizar, 2022). Scams represent blatant betrayals of trust, and it is suspected that powerful organisations exploit victims' overconfidence or excessive trust when they do not appear vulnerable (Laroche et al., 2018).

One contributing factor to online scams is the lack of awareness and education or knowledge among the public, including civil servants, regarding fraud prevention and the various types of scams (AFC Thoughts, 2024). Basyir and Harun (2022) noted that low awareness of cybercrime significantly contributes to the increasing cases of online scams. Many people and businesses are vulnerable to scams because they are ignorant of the different kinds of fraud and the strategies used by scammers. Due to the expansion of the digital economy and the increasing reliance on online transactions, scammers now have more opportunities to take advantage of weak systems and people. The emergence of cyber fraud has been further aided by weak cybersecurity protections and insufficient personal data protection.

Moreover, research on online scams in Malaysia is limited, particularly regarding romance scams, which remain underexplored despite the increasing number of reported cases. Much empirical research has examined the characteristics that influence people's compliance with scams, particularly in light of the rise in online scams (Fischer et al., 2013; Whitty, 2020; Buchanan & Whitty, 2013; Kirwan et al., 2018; Quek, 2023). Even though many government and organization websites provide information on how to avoid scams, victimization incidents are increasing. Online fraud has not been effectively mitigated by strategies that only concentrate on comprehending the traits of scam victims. Thus, a change of viewpoint is desperately needed in order to investigate the elements that help people stay away from online scams. Prior studies 60 (Whitty 2018; Ullah et al., 2019; Coluccia et al., 2020; Hanoch & Wood, 2021) have shown that scam victims are more likely to be middle-aged, which is often described as people between the ages of 40 and 60 which is describes as a stable group income (Britannica, 2023). This group frequently has comparatively more money to spend (Whitty, 2018; Yu et al., 2022). There is a research gap, though, as there are not many studies conducted focusing on online scam awareness study focus on civil servants in the Malaysian context are limited, highlighting a research gap. Existing research (Mohd Padil et al., 2022; Mohd Zaharon et al., 2021; Jusoh & Nizar, 2022) primarily targets the younger generation. Consequently, this study aims to address this gap by investigating the influential factors affecting online scam awareness among Malaysian civil servant particularly in the light of increasing number of online scams.

2.0 Literature Review

Online scam awareness can be defined as the ability to recognize, understand, and respond to fraudulent schemes in the digital domain. Ramadhan (2022) defines online scam awareness as the extent of knowledge and understanding regarding deceptive practices, which includes detecting warning signs and assessing risks associated with scams. Similarly, Zahari et al. (2019) and Yoon (2002) emphasize that online scam awareness involves understanding one's level of risk and having factual knowledge about scams. This involves being able to recognize the deceptive strategies used by scammers, evaluate the warning indications and indicators that are usually connected to these types of scams, and react appropriately to such internet frauds. Since scam awareness aims to understand the characteristics and sources of fraud, it is an essential part of scam control. This knowledge is essential because it helps people become less susceptible to scams by raising awareness of how important it is to avoid them (Astriana & Adhariani, 2019). This includes awareness when purchasing products online, for instance. One needs to identify the level of online scam awareness to understand one's level of risk and have knowledge of the facts (Zahari et al., 2019).

Numerous types of online scams occur daily, and the problem will never be resolved if internet users are unaware of them and lack knowledge about them. According to research by Gottschalk and Hamerton (2022), there are ways to prevent online scams, but no progress will be made in this area until everyone knows how to use the Internet responsibly. There are many kinds of scams that happen online, such as phishing, phone calls, video scams, and identity theft.

Due to people's increasing reliance on advanced technology, they use the internet more often for socialising in both personal and professional contexts, including daily interactions, work, and online services (banking, education, and virtual healthcare, etc.). Due to the advent of the internet and advanced technologies, even the way businesses operate in this field has changed. Without a doubt, the Internet has been the fastest-growing mode of communication over the past few decades (Patel & Binjola, 2020). This indicates that the development of information technology has contributed to a significant increase in Internet usage. Continuous connectivity increases cyber security risks, which may include threats to critical infrastructure and the economy. Individual internet users may face cybersecurity threats to their privacy, identity, and confidential information (Okereafor & Adebola, 2020). In addition, there are risks associated with Internet use that are explicitly related to cybersex, pornography, the exposure of personal information, cyberaddiction, online scam, and gambling addiction (Rahman et al., 2020). The authors of the study, Ngo et al. (2020), emphasised cyberspace's contribution to daily life by stating, "In our technology- and information-infused world, cyberspace is an integral part of contemporary society. Cyberspace enables and greatly facilitates most people's personal and professional digitally mediated activities daily. According to a different study by Zwilling et al. (2022), most internet users are still inadequately informed about the various online threats and cybercrimes.

According to Mokhsin et al. (2018), Malaysia is listed among one of the countries or cities or regions that have a high-risk for online scam. The environment of the social media applications enable scammer to trap their victims through a fake profile without being traced. The scammer trapped victims to make payments but never sent them the goods they already paid for. The number of reports received regarding online shopping scam has increased as the popularity of online shopping and online auctions keeps growing. Most complaints involve not receiving the paid-for products, receiving them late, receiving non-original or different products than advertised, or not receiving the terms and conditions that should have been included with the purchase (Malaysian Digest, 2015).

3.0 Methodology

This study utilizes quantitative research methods with a non-probability sampling approach. Sample units were selected from the population through purposive, or judgmental sampling. The primary aim of this technique is to create a sample that accurately represents the population (Lavrakas, 2008; Shafira, A., & Mayangsari, L., 2020). The respondents of this study a civil servant. According to the Department of Statistics Malaysia (DOSM), there were 1,260,429 permanent civil servants as of March 30, 2024.

To determine the appropriate sample size for this study, the researcher employed G*Power 3.1.9.7 software to conduct a priori power analysis for multiple linear regression analysis (fixed model, R^2 deviation from zero). The analysis aimed to detect a medium effect size ($f^2 = 0.15$) with a significant level (α) of 0.05 and a power level ($1–\beta$) of 0.80, using three predictors. Based on these parameters, the minimum required sample size was calculated to be 77 respondents, providing sufficient power (80.17%) to detect meaningful relationships among variables in this model. According to Baruch and Holtom (2008), the average response rate for data collected from individuals is 52.7%. Therefore, the bigger sample size was also an attempt at improving the number of responses for this study to enable the results to be more generalizable to the population. Hence the total respondent of this study is 144 respondents. The dependent variable is online scam awareness, while the independent variables are attitude, knowledge and environment (Refer figure 1).

Data collection was conducted using a questionnaire divided into five sections. The first section was the respondents' demographics, such as gender, age, education level, employer type, service group, household income, length of service and experience with online scams. The second section focused on online scam awareness, the dependent variable. The third, fourth and fifth sections addressed the independent variables: attitude, knowledge and environment respectively. These sections used the 5-point Likert scale, with responses ranging from 1(strongly disagree) to 5 (strongly agree). The variables and their measurement intervals were based on prior studies by Zakiah Saizan & Dalbir Singh (2018).

The questionnaire was created using Google form and the links were distributed to the 144 civil servants in the sample via WhatsApp. All responses were complete and valid, with no missing values. Subsequently, the collected data were analyzed using SPSS software to perform the descriptive statistical analyses

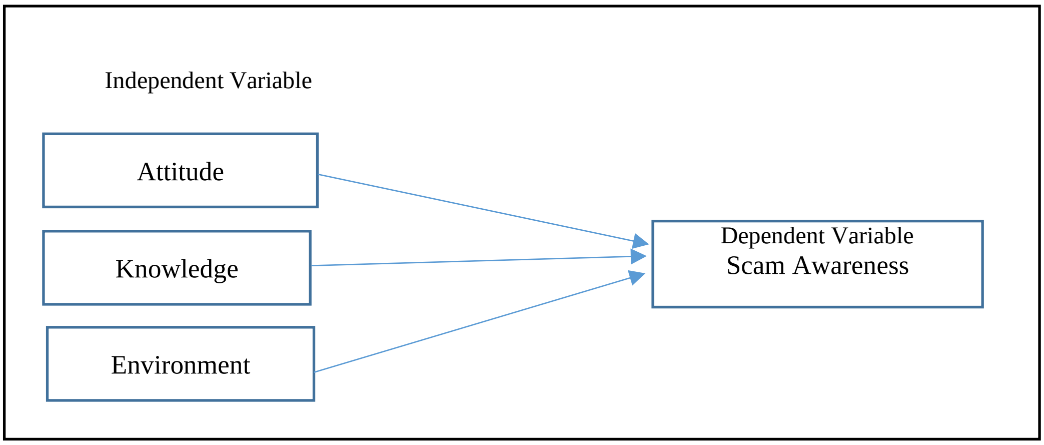

Figure 1*: Research Framework*

4.0 Data Analysis and Findings

In this study, the collected data were analyzed using the Statistical Package for the Social Sciences (SPSS) Version 26.0.

Descriptive Analysis

To describe the demographic profile of the respondents, the frequency and percentage distributions were used. A total of 144 valid responses were collected and used for descriptive analysis.

Respondent’s Profile

Table 1 presents the demographic characteristics of the respondents, which includes gender, age, education level, employer type, service group, household income, length of service, and experience with online scams.

Table 1
Respondents' Profile

Characteristics		Frequency (n=144)	Percentage
Gender	Male	54	37.5
	Female	90	62.5
Age	20 – 29 years old	4	2.8
	30 – 39 years old	37	25.7
	40 – 49 years old	75	52.1
	50- 60 years old	28	19.4
Education Level	Sijil Pendidikan Malaysia (SPM)	18	12.5
	Diploma/ STPM	34	23.6
	Degree	37	25.7
	Master	47	32.6
	PhD	8	5.6
Employer	Federal	138	95.8
	States	6	4.2
Service Group	Management & Professional (Grade 41 and above)	83	57.6
	Implementation (Grade 29 and above)	32	22.2
	Support Staff (Grade 19 and below)	29	20.1
Household Income	RM 2500 and below	10	6.9
	RM 2501 – RM4500	29	20.1
	RM4501 – RM6500	29	20.1
	RM6501 – RM8500	25	17.4
	RM8501 -RM10500	24	16.7
	RM10501 and above	27	18.8
Length of Service	10 years and below	21	14.6
	11 years – 20 years	73	50.7
	21 – 30 years	40	27.8
	31 years and above	10	6.9
Experience with online scam	Victim of a scam	18	12.5
	Attempted scam	111	77.1
	No experience	15	10.4
Types of Scam Experienced	Phishing	17	11.8
	Telephone call	95	66
	Video scam	4	2.8
	Theft Identity	11	7.6
	Not applicable	17	11.8
Reported Financial Loss	No financial loss	123	85.4
	RM5000 and below	17	11.8
	RM 5001 – RM10,000	2	1.4
	RM10 001 and above	2	1.4

Refer to Table 1, 144 participants participated in this study. The majority of the respondents were female (62.5%), which is 90 respondents, while the total number of male respondents was 54 respondents (37.5%), and most of them were aged 40 -49 years old (521%). There was a total of 37 people between the ages of 30-39, while only 4 of the respondents were aged 20-29 years old. Most respondents, 47 individuals, had master level of education, 37 of them had degree, 34 of the respondents had a diploma, 18 had a minimum level of education, which is SPM, and 8 of the respondents had the highest level of education, which is PhD. For household income, a total of 29 respondents has an income at level RM 2500 to RM4500 and RM4501 – RM6500, 27 people have an income at the level of RM10501 and above, 25 people have an income at the level of RMRM6501 – RM8500, 24 people have an income at the level of RM8501 – RM10,500, 10 people have an income at the level of RM2501 and below. For length of service, 73 of respondents have 11- 20 years of service, 40 of the respondents have 21 – 30 years of service, 21 of the respondents have 10 years and below and 10 of the respondents have 31 years and above of service. Meanwhile, for the experience of being involved with online scam, a total of 113 respondents had experience attempted scams, 18 of the respondents have been a victim of online scam and only 15 of the respondents have no experience of online scam. A total of 21 respondents of this study have been victims of online scam and involved financial losses, whereby 17 people suffered a financial loss of RM 5000 and below, two people suffered a financial loss of RM 5001 -RM10,000 and 2 people suffered a financial loss of RM10,001 and upward.

Descriptive Analysis

Descriptive statistics were used to determine the level of online scam awareness and the influence of attitude, knowledge and environment as independent variables. The results indicated that most of the civil servants had a very high level of online scam awareness (mean: 4.398, SD: 0.652) indicating a strong understanding of how to identify and report online scam attempts. The knowledge level was also high (mean: 4.012; SD:0.634), followed by a high rating for environment influence (mean: 3.615; SD:0.822). The attitude variable scored a moderate influence (mean: 3.202; SD:0.555), suggesting that while awareness and knowledge were high, behavioral attitude towards online scams were moderate and may need further attention in awareness campaigns.

Table 2
Mean Score Interpretation Table

Variable	N	Mean	SD	Interpretation
Scam Awareness	144	4.398	0.652	Very high
Attitude	144	3.202	0.555	Medium
Knowledge	144	4.0121	0.634	High
Environment	144	3.615	0.822	High

5.0 Discussion and Conclusions

The findings of this study incate that civil servants possess a high level of awareness regarding online scams, which is the mean score is 4.398. This suggests that they are generally knowledgeable about online theats and know the right channels to report scam attempts. The high awarenss level can be attributed to widespread campaigns, training and increase media coverage on digital safety. Factors such as knowledge, environment and attitude found have an influence on online scam awareness. Knowledge and environment have a high mean (4.012) and (3.615) respectively. This indicates that civil servants have a knowledge on online scams and they are informed about online security threats. They are also influenced by surroundings such as workplace policies, peer discussions or organizational initiatives in cultivating scam awareness.

However, the attitude variable scored were moderate (mean: 3.202), suggesting that despite having knowledge and awareness, there may still a gap in personal commitment or behaviour towards online safety. Some civil servants may not perceive themselves as vulnerable to online scams threats, thus leads them to underestimate the importance of preventive actions. Notably, 77.1% of the respondents reported experiencing attempted scams and 12.5% became victims. These facts show that online scam threats are real and prevalent even among knowledgeable individuals. The most common type scam was through telephone calls (66%) indicating that traditional scam techniques remain highly effective, particularly when scammers impersonate trusted entities.

This study concludes that while civil servants in Malaysia demostrate a high level of awareness and knowledge about online scams, actual exposure to scam attempts remain significantly high. Thus, identifying other factors that may influece the level of scam awareness is necceties. Furthermore, this study also my extend to longitudinal approach on behavioral change in order to evaluate the long-term effectiveness of awarenss campaigns and policy implementation in gornment institutions or policy.

REFERENCES

AFC Thoughts. (2024). Top Transaction Fraud Scenarios in Asean. Tookitaki.com. Retrieved https://www.tookitaki.com/compliance-hub/top-fraud-detection-and-prevention-solutions-explored

Baruch, Y., & Holtom, B.C. (2008). Survey response rate levels and trends in organizational research. Human Relations, 61(8), 1139-1160. https:// doi.org/10.1177/0018726708094863

Basyir, M. & Harun, H.N. (2022, September 26). Online Scam Cases Increasing in Malaysia. New Straits Times. http://www.nst.com.my/news/nation/2022/09/834531/online-scam-cases-increasing-malaysia.

Buchanan, T., & Whitty, M. T. (2013). The online dating romance scam: Causes and consequences of victimhood. Psychology, Crime & Law, 20(3), 261– 283.

Burton, A., Cooper, C., Dar, A., Mathews, L., & Tripathi, K. (2021). Exploring how, why and in what contexts older adults are at risk of financial cybercrime victimisation: A realist review. *Experimental Gerontology*, 111678.

Button, M., Nicholls, C. M., Kerr, J., & Owen, R. (2014). Online frauds: Learning from victims why they fall for these scams. Australian & New Zealand Journal of Criminology, 47(3), 391–408.

Cross, C., & Blackshaw, D. (2014). Improving the Police Response to Online Fraud. Policing, 9(2), 119–128

Fischer, P., Lea, S. E. G., & Evans, K. M. (2013). Why do individuals respond to fraudulent scam communications and lose money? The psychological determinants of scam compliance. Journal of Applied Social Psychology, 43(10), 2060–2072.

Gainsbury, S. M., Browne, M., & Rockloff, M. (2019). Identifying risky Internet use: Associating negative online experience with specific online behaviours. *New Media & Society*, *21*(6), 1232-1252.

Geldenhuys, K. (2022). Paying to get a job Employment scams. *Servamus Community-based Safety and Security Magazine*, *115*(8), 30-34.

Gottschalk, P., & Hamerton, C. (2022). Technology Issues. In *White-Collar Crime Online* (pp. 149-174). Palgrave Macmillan, Cham.

Hidayath Hisham. Malaysia records RM1.2b losses due to Online Scams. The Malaysian Reserve. December 3, 2024. Retrieved on 12 April 2025. https://themalaysianreserve.com/2024/12/03/malaysia-records-rm1-2b-losses-due-to-online-scams/

Jusoh, W. N. H. W., & Nizar, N. M. S. (2022). Online Scams Awareness Among Muslim University Students in Malaysia. *Journal of Islamic*, *7*(43).

Kirwan, G. H., Fullwood, C., & Rooney, B. (2018). Risk Factors for Social Networking Site Scam Victimization Among Malaysian Students. Cyberpsychology, Behavior, and Social Networking, 21(2), 123–128.

Lin, K., Wu, Y., Sun, I. Y., & Qu, J. (2023). Telecommunication and cyber fraud victimization among Chinese college students: An application of routine activity theory. Criminology & Criminal Justice, 174889582211461. https://doi.org/10.1177/17488958221146144

Ministry of Communications and Digital. (2022, March 10). KKMM. https://www.kkd.gov.my/en/public/news/21562-bukit-aman-over-90-000- online-fraud-cases-from-2017-2021-involving-rm3-3b-losses

Mohd Padil, H., Kasim, E. S., Muda, S., Ismail, N., & Md Zin, N. (2022). Financial literacy and awareness of investment scams among university students. Journal of Financial Crime, 29(1), 355-367

Mohd Zaharon, N. F., Mohd Ali, M., & Hasnan, S. (2021). Factors Affecting Awareness of Phishing Among Generation Y. Asia-Pacific Management Accounting Journal, 16(2), 409–444.

Mokhsin, M., Aziz, A. A., Zainol, A. S., Humaidi, N., & Zaini, N. A. A. (2018). Probability Model: Malaysian Consumer Online Shopping Behavior towards Online Shopping Scam. *International Journal of Academic Research in Business and Social Sciences*, *8*(11), 1529-1538.

Moidunny, K. (2009). The Effectiveness of the National Qualifications Professional Qualification Program (NPQH). Doctor of Philosophy, Selangor: Faculty of Education, Universiti Kebangsaan Malaysia.

Ngo, F. T., Piquero, A. R., LaPrade, J., & Duong, B. (2020). Victimization in cyberspace: Is it how long we spend online, what we do online, or what we post online?. *Criminal justice review*, *45*(4), 430-451.

Okereafor, K., & Adebola, O. (2020). Tackling the cybersecurity impacts of the coronavirus outbreak as a challenge to internet safety. *Int J IT Eng*, *8*(2).

Patel, K., & Binjola, H. (2020). Tik Tok the New Alternative Media for Youngsters for Online Sharing of Talent: An Analytical Study. *Available at SSRN 3600119*.

Quek, H. L. (2023). *Influential factors of online scam awareness among generation X in Malaysia* (Doctoral dissertation, UTAR).

Rahman, N., Sairi, I., Zizi, N. A. M., & Khalid, F. (2020). The importance of cybersecurity education in school. *International Journal of Information and Education Technology*, *10*(5), 378-382.

Ramadhan, D. (2022). Strengthening Integrity and Fraud Awareness in Preventing Fraud During the Covid-19 Pandemic. Asia Pacific Fraud Journal, 7(2), 213.

Salih, K. O. M., Rashid, T. A., Radovanovic, D., & Bacanin, N. (2022). A comprehensive survey on the Internet of Things with the industrial marketplace. *Sensors*, *22*(3), 730.

Telenor Group (2016). Asia's Top Internet Scams and How to Stay Safe: Telenor Group Study underscores the importance of protecting personal information online. *Retrieved from* https://www.telenor.com/asias-top-internet-scams-and-how-to-stay-safe/.

The Star. (2023, May 26). Malaysia recorded a significant rise in online fraud cases since 2020, says SC chairman. The Star. https://www.thestar.com.my/news/nation/2023/05/26/malaysia-recordssignificant-rise-in-online-fraud-cases

Whitty, M. T. (2020). Is There a Scam for Everyone? Psychologically Profiling Cyberscam Victims. European Journal on Criminal Policy and Research, 26(3), 399–409.

Saizan, Zakiah. (2018). Cyber Security Awareness among Social Media Users: Case Study in German-Malaysian Institute (GMI). Asia-Pacific Journal of Information Technology & Multimedia. 07. 111-127. 10.17576/apjitm-2018-0702(02)-10.

Zahari, A. I., Bilu, R., & Said, J. (2019). The Role of Familiarity, Trust And Awareness Towards Online Fraud. *Journal of Research and Opinion*, *6*(9), 2470-2480.

Zhang, C., Liu, L., Zhou, S., Feng, J., Chen, J., & Xiao, L. (2022). Contact-Fraud Victimization among Urban Seniors: An Analysis of Multilevel Influencing Factors. *ISPRS International Journal of Geo-Information*, *11*(3), 201.

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber security awareness, knowledge and behavior: a comparative study. *Journal of Computer Information Systems*, *62*(1), 82-97