Available Online at www.e-iph.co.uk
Indexed in Clarivate Analytics WoS, and ScienceOPEN

E-B Environment - Behaviour Proceedings Journal

AcE-Bs2023KualaTerengganu

https://www.amerabra.org

e-IPH e-International Publishing House Ltd., United Kingdom

11th ASIAN Conference on Environment-Behaviour Studies
Primula Beach Hotel, Kuala Terengganu, Malaysia, 14-16 Jul 2023

Cyber Hygiene Practices from The Lens of Professional Youth in Malaysia

Amily Fikry[1*], Muhammad Iskandar Hamzah[1], Zuhal Hussein[2], Didin Hadi Saputra[3]
** Corresponding Author*

[1] Faculty of Business and Management, Universiti Teknologi MARA Puncak Alam, Malaysia
[2] Faculty of Business and Management, Universiti Teknologi MARA Kelantan, Malaysia
[3] Faculty of Administrative Science, University of Nahdatul Wathan Mataram, Kaktus Street, No.1-3, West Nusa Tenggara, Indonesia.

amily@uitm.edu.my, iskandarh@uitm.edu.my, zuhal@uitm.edu.my, didinhs@unwmataram.ac.id

Abstract
Researchers have recognized cyber hygiene as an essential factor in reducing cybersecurity breaches. Factors affecting cyber hygiene practices are cyber hygiene knowledge and demographic factors. Inconclusive research has been found to be concerned with the extent of expertise and demographic factors that may affect cyber hygiene practices. This current pilot study aims to diagnose the effect of knowledge and demographic factors on cyber hygiene practices among professional youth in Malaysia. Forty-one usable questionnaires were further analyzed. The result showed no significant differences between demographic factors and cyber hygiene practices; and no significant relationship between knowledge and cyber hygiene practices among professional youth in Malaysia.

Keywords: Keywords: Cyber hygiene; cybersecurity; youth; professional

DOI: https://doi.org/10.21834/e-bpj.v8i25.4827

1.0 Introduction

Data protection and privacy systems in Malaysia have had a poor reputation. In the year 2019, Malaysia ranked fifth-lowest out of 47 countries in terms of the matter at hand. Additionally, Malaysia had previously suffered from severe data leaks. Reports from MyCERT (Malaysia Computer Emergency Response Team) revealed an escalating number of cyberattack cases in Malaysia between 2008 and 2020.

Past research have recognized cyber hygiene as an essential factor in reducing cybersecurity breaches. Cyber hygiene is an adaptive behaviour to mitigate risky online activities that can put an individual's information at risk. Cyber hygiene practices protect the safety and integrity of online users' personal information on their Internet-enabled devices from being compromised in a cyberattack.

In the same vein, it is further noted that human is the weakest link in the cybersecurity chain (Anwar et al., 2017), while human interpersonal factor (demographic factor) shapes an individual's perception, attitude, and performance. Thus, it is timely to understand human security behaviour (specifically concerning cyber hygiene practices) from the interpersonal factor perspective, namely gender, educational level, professional level, age, and knowledge (Nosek, Banaji & Greenwald, 2002). Al-Hawamleh (2023) further highlighted that research on these interpersonal factors (demographic factors) are crucial to be focused on, but have to be adequately explored.

As noted above, one of the interpersonal factors (demographic factors) that may affect cyber hygiene practices is cyber hygiene knowledge. Cyber hygiene knowledge shapes individuals' behaviour, especially in public places such as office workspaces. Past researchers discovered that those with high cyber knowledge attempt to treat cyberattack seriously, thus becoming very cautious when

eISSN: 2398-4287 © 2023. The Authors. Published for AMER & cE-Bs by e-International Publishing House, Ltd., UK. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/). Peer–review under responsibility of AMER (Association of Malaysian Environment-Behaviour Researchers), and cE-Bs (Centre for Environment-Behaviour Studies), College of Built Environment, Universiti Teknologi MARA, Malaysia.
DOI: https://doi.org/10.21834/e-bpj.v8i25.4827

accessing the internet (Alsulami et al., 2021; Kennison & Chan-Tin, 2020). Knowledgeable employees tend to be more careful, taking precautionary steps to avoid or reduce the chances of cybersecurity threats.
On the other hand, past research found inconclusive findings concerning the extent of interpersonal factors, mainly demographic factors (gender, educational level, professional level, age) that may affect cyber hygiene practices (Fatokun et al., 2019; Kshetri & Chhetri, 2022; Herath, Khanna & Ahmed, 2022; Adholiya & Adholiya, 2019). Therefore, this paper aims to diagnose the effect of knowledge and demographic factors on cyber hygiene practices among professional youth in Malaysia.

2.0 Literature Review

Human is the weakest link in the cybersecurity chain (Anwar et al., 2017). It is crucial to understand human security behaviour with demographic factors (gender, educational level, professional level, age, knowledge). Nosek, Banaji, and Greenwald (2002) further noted that the demographic factor is one of the fundamental groups that profoundly influence an individual's perception, attitude, and performance (Ibrahim, Saharudin & Lestari, 2023). Therefore, to encourage good cyber hygiene practices among professional youth, it is crucial to understand the interpersonal factor (demographic factor) of these professional youth employees.

Past studies usually associated the usage of information technology with interpersonal factors such as gender, age, educational level, and professional level (Muhammad et al., 2023; Fikry & Bustami, 2011), which directly affect cyber hygiene practices. They mainly believed that a person of male gender, aged between 20 and 35, tends to use more information technology. As a result, these groups (males aged between 20 and 35 years old) take more cybersecurity risks than their counterparts (Shah & Agarwal, 2020).

However, by looking at cyber hygiene practices in different research locations, past researchers have also discovered that demographic factors such as gender, age, and education level are not important predictors of cyber hygiene practices (Anwar et al., 2017; Herath, Khanna & Ahmed, 2022; Alsulami et al., 2021). From a Malaysian perspective, Fatokun et al. (2019) discovered that age and gender affect cyber hygiene practices, whilst academic qualification does not have significant differences in cyber hygiene practices.

In line with that, Kshetri and Chhetri (2022) believed that gender asymmetry is a significant predictor of cyber hygiene practices. In another, inconclusive findings were reported by Adholiya and Adholiya (2019) regarding demographic factors towards cyber hygiene practices. Hence, it is further postulated that:

H1: There are significant differences between age and cyber hygiene practices.
H2: There are significant differences between gender and cyber hygiene practices.
H3: There are significant differences between professional level and cyber hygiene practices.
H4: There are significant differences between educational level and cyber hygiene practices.

Past researchers have also revealed that knowledge significantly predicts cyber hygiene practices (Alsulami et al., 2021; Kennison & Chan-Tin, 2020; Shojaifar, Fricker & Gwerder, 2020). This reflects that knowledge affects professional youths' cyber hygiene practices, whereby the more knowledgeable they are, especially knowledge related to cyber security; they will take more precautious measures in an attempt to avoid or reduce the prevalence of security breaches. A person that possesses information technology knowledge (knowledgeable) practises good cyber hygiene. Al-Hawamleh (2023) agreed with the notion above and further added that these professional employees should have a full grasp of cybersecurity knowledge, especially in the area of common attack methods and the use of cybersecurity software.

Meanwhile, Alharbi et al. (2021) discovered that professional employees with more cyber security knowledge tend to practise poor cyber hygiene, especially concerning losing an organization's sensitive data. Haeussinger & Kranz (2017) further argued that knowledge may be a double-edged sword as information technology knowledge enables employees to manipulate an organization's cyber security policy or even engage in fraudulent cyber security behaviour. However, contradictory findings exist regarding the relationship between knowledge and cyber hygiene practices. Although organizational employees have cyber security knowledge, no action is taken to practise good cyber hygiene. In this situation, implementing rewards and punishment is required to ensure good cyber hygiene is being practised among employees (Gundu, 2019). Hence, this research posited the following hypothesis:

H5: There is a significant relationship between knowledge and cyber hygiene practices.

3.0 Methodology

This section covers on matters in terms of samples, research instruments, respondent selection, and questionnaire distribution.
This research focused on professional youth respondents. Data were collected using purposive sampling. The sample was selected based on those who fulfilled the criteria set by the researchers: youth aged 20 to 35 years old, working in either executive or managerial level in an organization.

The criteria mentioned above were set in the screening question. Screening questions were used to select respondents that fit the purpose of the study, mainly professional youth. Those who have not fulfilled the criteria set (aged between 20 and 35 years old, working in either executive or managerial level in an organization) in the screening question, were eliminated and were not required to answer the remaining questionnaire. For this pilot study, only those aged 20-35 years old, working at the executive or managerial level, were categorized as professional youth.

Questionnaires were distributed using SurveyMonkey Audience, and analyses were done using IBM SPSS 28. Items to measure knowledge was adopted from Parsons et al. (2017), while items to measure cyber hygiene practices were adopted from Anwar et al. (2017), Vance, Siponen and Pahnila (2012); Shih, Lin, Chiang and Shih (2008); Davidson and Sillence (2010) as well as Ng, Kankanhalli and Xu (2009).

4.0 Findings

This section discusses the findings of the research. Out of 87 questionnaires distributed, only 41 usable questionnaires were collected and further analyzed. The remaining 46 questionnaires were omitted as they did not fall under the category of professional youth (age of respondents below 20 years old or above 35 years old; respondent's occupation did not fall under the executive, managerial or professional levels).

4.1 Demographic Profiling of Respondents

Table 1 shows the demographic data of the respondents. Twenty respondents representing 48.78% of the respondents, were male, and 21 respondents representing 51.22% were female. The respondents were categorized into five different phases of age. Eight respondents (19.51%) of the respondents were between 20 and 25 years old; 12 respondents (29.27%) were between 26 and 30 years old; the highest frequency of 21 respondents (51.22%) were between 31 and 35 years old and none of the respondents were above 35 years old.

At the current occupational level, there are three levels to represent the respondents. The highest frequency of 25 respondents (60.98%) were working at the executive level, and 16 respondents (39.02%) were working at a managerial level. None of the respondents were working in the clerical class.

Looking at the highest academic qualification of respondents, the majority of them earned Bachelor's degree (92.68%, 38 respondents). In contrast, the remaining respondents (16 respondents) obtained postgraduate degrees, namely Master/Ph.D./Doctor of Business Administration (39.02%). None of the respondents selected earned SPM/STPM or below and Certificate/Diploma.

In analysing the respondent's residential state, the majority of them reside in Kuala Lumpur (36.59%, 15 respondents), followed by Selangor (29.27%, 12 respondents), Sabah (12.20%, five respondents), Pulau Pinang (2.44%, one respondent), Johor (7.32%, three respondents), Kelantan (2.44%, one respondent), Terengganu (4.88%, two respondents), Melaka (2.44%, one respondent) and Sarawak (2.44%, one respondent) respectively.

Table 1: Demographic Profile of Respondents

Demographic Factor	Frequency	Percentage (%)
Gender		
Male	20	48.78
Female	21	51.22
Total	41	100
Age		
Under 20 years old	0	0
20-25 years old	8	19.51
26-30 years old	12	29.27
31-35 years old	21	51.22
Above 35 years old	0	0
Total	41	100
Academic qualification		
SPM/STPM or below	0	0
Certificate/Diploma	0	0
Bachelor's Degree	38	92.68
Master/PhD/Doctor of Business Administration	3	7.32
Total	41	100
Current Occupational Level		
Clerical Level	0	0
Executive Level	25	60.98
Managerial Level	16	39.02
Total	41	100
Residential State		
Selangor	12	29.27
Kuala Lumpur	15	36.59
Pulau Pinang	1	2.44
Perlis	0	0
Kedah	0	0
Johor	3	7.32
Kelantan	1	2.44
Terengganu	2	4.88
Melaka	1	2.44
Negeri Sembilan	0	0

Sabah	5	12.20
Sarawak	1	2.44
Total	41	100

4.2 Hypotheses testing

This subsection elaborates on the analyses of the hypotheses. Based on the analyses conducted, it has been found that:

H1: There are significant differences between age and cyber hygiene practices.

A one-way between-group analysis of variance was conducted to explore the effect of age on cyber hygiene practices. Subjects were divided into four groups according to age (Group 1: 20-25 years old, Group 2: 26-30 years old, Group 3: 31-35 years old, Group 4: above 35 years old). There were no significant differences at the < .05 level in cyber hygiene practices for the four age groups: F (3, 37) = 0.477, p = 0.7. Thus, H1 was rejected.

H2: There are significant differences between gender and cyber hygiene practices.

An independent sample t-test was conducted to compare the cyber hygiene practices for males and females. There were no significant differences in scores for males (M=1.86, SD= 0.3844) and females (M=1.70, SD=0.70; t(39) = 0.871, p=0.389 (two-tailed). The magnitude of differences in the means (mean difference = 0.15524, 95% CI: -0.20536 to 0.51584) was very small (eta squared = 0.019). Thus, H2 was rejected.

H3: There are significant differences between professional level and cyber hygiene practices.

A one-way between-group analysis of variance was conducted to explore the effect of professional level on cyber hygiene practices. The subjects were divided into two groups according to their professional level (Group 1: executive level and Group 2: managerial level). There were no significant differences at the p< .05 level in cyber hygiene practices for the two groups: F (1, 39) = 0.539, p = 0.467. Thus, H3 was rejected.

H4: There are significant differences between educational level and cyber hygiene practices.

A one-way between-group analysis of variance was conducted to explore the effect of educational level on cyber hygiene practices. The subjects were divided into two groups according to their professional level (Group 1: Bachelor's degree and Group 2: Master/PhD/DBA). There were no significant differences at the p< .05 level in cyber hygiene practices for the two groups: F (1, 39) = 0.004, p = 0.952. Thus, H4 was rejected.

H5: There is a significant relationship between knowledge and cyber hygiene practices.

The regression analyses were conducted between knowledge and cyber hygiene practices. The findings indicated that the R2 was 0.054, F (1, 39) = 2.236, p>0.10, indicating that 5.4 per cent of the variance in cyber hygiene practices was explained by knowledge. A closer examination revealed that knowledge (β = 0.233, p> 0.10) was not significantly related to cyber hygiene practices. Thus, H5 was rejected.

5.0 Discussion and Conclusion

This section elaborates on the research's discussion, conclusion and limitations.

The findings revealed no significant differences between the professional level of employees and cyber hygiene practices, which contradicts past research (Sadok, Alter & Bednar, 2020 Sarkar et al., 2020; Hedstrom et al., 2011). Employees' professional level may not be a significant predictor in measuring cyber hygiene practices. Participation of these professional employees in developing cyber security guidelines and frameworks for the company may motivate them to practise good cyber hygiene (Sadok, Alter & Bednar, 2020).

The findings showed no significant differences between educational level and cyber hygiene practices and no significant relationship between knowledge and cyber hygiene practices. These findings reflected weak cyber security culture in the organizations. A good cyber security culture will inculcate employees to naturally practise good cyber hygiene in their daily office tasks and vice versa (Uchendu et al., 2021). Employees do not prioritize cyber security and do not receive sufficient training or resources to implement a good cyber hygiene practice. A weak cyber security culture will result in poor cyber hygiene practices, regardless of employee's educational level.

In line with that, the security knowledge possessed by employees in the organization is also a key part of cyber security culture. Employees who do not possess sufficient cyber security knowledge will practice poor cyber hygiene in their organization (Van Niekerk & Von Solms, 2010). As a result, cyber security knowledge is important, and having such knowledge will certainly affect employees' cyber hygiene practices (Alharbi et al., 2021). In contrary, the findings of this research revealed no significant relationship between knowledge and cyber hygiene practices. This may be due to the reason that employees may not fully grasp the risks associated with certain online behaviours or actions (Kure, Islam, & Razzaque, 2018). This could lead them to engage in potentially risky behaviours without realizing the consequences.

Past studies showed that there have been age and gender differences in technology adoption and technology usage (Morris, Venkatesh, & Ackerman, 2005) and security compliance (Vance, Siponen, & Pahnila, 2012; Ifinedo, 2014), but the findings were not

consistent across studies (Anwar et al., 2017; Fatokun et al., 2019). On the other hand, this research discovered no significant differences between gender and age towards cyber hygiene practices.

The research findings revealed that demographic factors such as age, gender, educational level, professional level, and cyber hygiene knowledge are not the best predictor in measuring cyber hygiene practices among these professional youth. Other factors may be tested in the future to determine which factors are the best predictor for cyber hygiene practices.

Finally, there are several limitations in this research. Firstly, this research shows that demographic factors and cyber hygiene knowledge are not the best predictors in measuring cyber hygiene practices among these professional youth. Other factors, such as attitude and behaviour (Parsons et al., 2017), may be included as predictors by future researchers in cyber hygiene practices.

Second, this pilot research uses a small sample size (N=41); thus, results may vary when testing the same variables towards a larger sample size. A larger sample size may change the result (Chandrasekharan, Sreedharan, & Gopakumar, 2019; Shah & Agarwal, 2020). Third, the setting for this research is in Malaysia. Future researchers may use the same variable, to collect data in different countries where the result may vary.

Finally, future research may use open-ended questions in the survey or personal interviews with professional employees to assess their knowledge and experience with cyber hygiene practices. The present research has solely relied on the close-ended survey to obtain data from professional youth respondents.

Acknowledgment

The authors would like to acknowledge Universiti Teknologi MARA (UiTM) for the financial support through the Geran Penyelidikan MyRA, Project File No: 600-RMC 5/3/GPM (117/2022). Besides, the authors highly appreciate the faculty and team members for their excellent support in ensuring that this research is accomplished.

Paper Contribution to Related Field of Study

The results of this paper will assist the organization's cyber hygiene or cyber security unit in targeting the most crucial component in developing a cyber hygiene model and creating a cyber hygiene awareness programme for the organization's youth employees.

Based on the result of this research, disregard of age, education level, occupational level, gender, and knowledge; organizations and educational institutions need to design specific cyber hygiene training programmes that cater for professional youth to raise their awareness and to satisfy their unique needs in regards to cyber hygiene practices. However, other demographic variables (information technology literacy and usage, usage of public or private networks, subscription of internet plan, residential areas) may be used to test the significant differences in cyber hygiene practices. These variables, upon testing, may provide a good indicator in profiling the right target market to receive the right cyber security information disseminated by the organization. This will enable organizations to develop demographically-specific cybersecurity training and intervention programmes targeting the relevant constructs of the cyber hygiene model to improve the attitudes and behaviour of employees.

Furthermore, organizations that rely on training to create and increase awareness about good cyber hygiene practices, as a means to reduce cybersecurity threats, may use their employees' demographic factors to target training to individuals who are the most likely to engage in poor cyber hygiene practices. This may lead to a better return on investment for the organization (Kennison & Chan-Tin, 2020).

In another scenario, the effort to increase cyber hygiene knowledge among professional youth, organizations may consider conducting continuous training programmes to increase professional employees' awareness and expertise on updated information about cybersecurity issues such as those related to artificial intelligence (Al-Hawamleh, 2023).

Further to the above, organizations may consider disseminating information about cyber security using various media that suit the youth generation. For example, organizations may disseminate cyber hygiene information to professional youth using social media (Pham, Ulhaq, Nguyen, & Nkhoma, 2021) such as Twitter, Facebook, Tik Tok, and Instagram. This accordingly increases professional youth awareness and knowledge of cyber hygiene. Due to these social media contents being more attractive and engaging, hence these have become highly sought after among these youth generation.

References

Adholiya, A., & Adholiya, S. (2019). A Study on Cyber Security Practices and Tips Awareness among E-Banking Services Users of Udaipur, Rajasthan. Int. J. Sci. Res. in Multidisciplinary Studies Vol, 5(8).

Alharbi, F., Alsulami, M., Al-Solami, A., Al-Otaibi, Y., Al-Osimi, M., Al-Qanor, F., & Al-Otaibi, K. (2021). The impact of cybersecurity practices on cyberattack damage: The perspective of small enterprises in Saudi Arabia. Sensors, 21(20), 6901.

AL-Hawamleh, A. M. (2023). Predictions of Cybersecurity Experts on Future Cyber-Attacks and Related Cybersecurity Measures. International Journal of Advanced Computer Science and Applications, 14(2).

Alsulami, M. H., Alharbi, F. D., Almutairi, H. M., Almutairi, B. S., Alotaibi, M. M., Alanzi, M. E., Alotaibi, K. G., & Alharthi, S. S. (2021). Measuring awareness of social engineering in the educational sector in the Kingdom of Saudi Arabia. Information, 12(5), 208.

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. Computers in Human Behavior, 69, 437-443.

bt Fikry, A., & Bustami, M. R. (2011). The impact of demographics on the Malaysian teenager's influence towards family purchase decision of the game console. 2011 IEEE Colloquium on Humanities, Science, and Engineering,

Chandrasekharan, S., Sreedharan, J., & Gopakumar, A. (2019). Statistical issues in small and large samples: need of optimum upper bound for the sample size. International Journal of Computational and Theoretical Statistics, 6(2).

Davinson, N., and Sillence, E. (2010). It won't happen to me: Promoting secure behavior among Internet users. Computers in Human Behavior, 26(6), 1739-1747.

Fatokun, F., Hamid, S., Norman, A., & Fatokun, J. (2019). The impact of age, gender, and educational level on the cybersecurity behaviors of tertiary institution students: an empirical investigation on Malaysian universities. Journal of Physics: Conference Series,

Gundu, T. (2019). Acknowledging and reducing the knowing and doing gap in employee cybersecurity compliance. ICCWS 2019 14th International Conference on Cyber Warfare and Security,

Haeussinger, F., & Kranz, J. (2017). Antecedents Of Employees' Information Security Awareness-Review, Synthesis, And Directions For Future Research.

Hedström, K., Kolkowska, E., Karlsson, F., & Allen, J. P. (2011). Value conflicts for information security management. The Journal of Strategic Information Systems, 20(4), 373-384.

Herath, T. B., Khanna, P., & Ahmed, M. (2022). Cybersecurity practices for social media users: a systematic literature review. Journal of Cybersecurity and Privacy, 2(1), 1-18.

Ibrahim, W. N. A., Saharudin, N. S., & Lestari, D. F. (2023). Knowledge, Attitude, and Practice of Computer Vision Syndrome among Office Workers in UiTM Puncak Alam. Environment-Behaviour Proceedings Journal, 8(24), 315-322.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. Computers & Security, 31(1), 83-95.

Kennison, S. M., & Chan-Tin, E. (2020). Taking risks with cybersecurity: Using knowledge and personal characteristics to predict self-reported cybersecurity behaviors. Frontiers in Psychology, 11, 546546.

Kure, H. I., Islam, S., & Razzaque, M. A. (2018). An integrated cyber security risk management approach for a cyber-physical system. Applied Sciences, 8(6), 898.

Kshetri, N., & Chhetri, M. (2022). Gender asymmetry in cybersecurity: socioeconomic causes and consequences. Computer, 55(2), 72-77.

Muhammad, N. S., Fikry, A., Hussein, Z., Hamzah, M. I., Sudarwanto, T., & Marlena, N. (2023). Are there Significant Differences between Gender and Education Level toward Trust, Image Appeal, Emotion, and Mobile Apps Environment?

Morris, M. G., Venkatesh, V., & Ackerman, P. L. (2005). Gender and age differences in employee decisions about new technology: An extension to the theory of planned behavior. IEEE Transactions on Engineering Management, 52(1), 69- 84.

Nosek, B. A., Banaji, M., & Greenwald, A. G. (2002). Harvesting implicit group attitudes and beliefs from a demonstration website. Group Dynamics: Theory, Research, and Practice, 6(1), 101.

Ng, B.Y., Kankanhalli, A., & Xu, Y. (2009). Studying users' computer security behavior using the health belief model. Decision Support Systems, 46(4), 815-825.

Pham, H. C., Ulhaq, I., Nguyen, M., & Nkhoma, M. (2021). An exploratory study of the effects of knowledge sharing methods on cyber security practice. Australasian Journal of Information Systems, 25.

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The human aspects of information security questionnaire (HAIS-Q): two further validation studies. Computers & Security, 66, 40-51.

Sadok, M., Alter, S., & Bednar, P. (2020). It is not my job: to explore the disconnect between corporate security policies and actual security practices in SMEs. Information & Computer Security, 28(3), 467-483.

Sarkar, S., Vance, A., Ramesh, B., Demestihas, M., & Wu, D. T. (2020). The influence of professional subculture on information security policy violations: A field study in a healthcare context. Information Systems Research, 31(4), 1240-1259.

Shah, P., & Agarwal, A. (2020). Cybersecurity behavior of smartphone users in India: an empirical analysis. Information & Computer Security, 28(2), 293-318.

Shojaifar, A., Fricker, S. A., & Gwerder, M. (2020). Automating the Communication of Cybersecurity Knowledge: Multi-Case Study. Information Security Education. Information Security in Action: 13th IFIP WG 11.8 World Conference, WISE 13, Maribor, Slovenia, September 21–23, 2020, Proceedings 13,

Shih, D. H., Lin, B., Chiang, H. S., & Shih, M. H. (2008). Security aspects of mobile phone virus: a critical survey. Industrial Management & Data Systems, 108(4), 478-494.

Uchendu, B., Nurse, J. R., Bada, M., & Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. Computers & Security, 109, 102387.

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS Security Compliance: Insights from Habit and Protection Motivation Theory. Information & Management, 49(3), 190- 198.

Van Niekerk, J., & Von Solms, R. (2010). Information security culture: A management perspective. Computers & Security, 29(4), 476-486.

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS Security Compliance: Insights from Habit and Protection Motivation Theory. Information & Management, 49(3), 190- 198.