

THE INFLUENCE OF PROTECTION MOTIVATION TO PROTECT THE SECURITY OF PERSONAL DATA AMONG YOUTH

¹Shariffah Mamat*, ²Wan Amizah Wan Mahmud, ³Arina Anis Azlan

¹Institute for Youth Research Malaysia (IYRES), Ministry of Youth and Sports
Malaysia

^{2&3}Centre for Research in Media and Communication (MENTION), Faculty of Social
Sciences and Humanities, National University of Malaysia (UKM), Malaysia

*Corresponding author: shariffah@iyres.gov.my

Published online: 30 November 2023

To cite this article: Mamat., S., W., Mahmud, W., A., Azlan, A., A., (2023). The Influence Of Protection Motivation To Protect The Security Of Personal Data Among Youth. *Asia Pacific Journal of Youth Studies (APJYS)*, 2(2), 95-114. <https://doi.org/10.56390/apjys2023.1.1.8>

To link to this article: <https://doi.org/10.56390/apjys2023.1.1.8>

ABSTRACT

The new norms during COVID-19 pandemic contributed to the increased usage of online mediums. Adaptation to the new norms as the country was hit by the COVID-19 pandemic was a catalyst for increased Internet usage. The behaviour of disclosing personal data in this careless virtual world is feared to increase the risk of becoming a victim of cyber threats. This article aims to display the findings of a study that focuses on protection motivation as a factor influencing youth behaviour to protect their data security when using the Internet. A total of 535 middle to late youth respondents (19-30 years old) from Putrajaya and Cyberjaya were selected by multistage random sampling. This quantitative study was conducted through online questionnaires from April to August 2021. The data collection process was conducted in compliance with the Standard Operating Procedures (SOP) under the Movement Control Order (MCO) which came into force during the period by the National Security Council (NSC). Data were analysed using Statistical Package for the Social Sciences (SPSS) version 25.0. Linear regression analysis is easy to use to analyse factors that influence Malaysian youth in protecting the security of personal data. The results of the study showed that threat assessment skills contributed significantly to threat coping skills, $F=1335.428$, $p < .000$. Threat assessment skills explained 84.5% of the variation in threat coping skills and became the primary predictor ($\beta = 1.268$, $p > .000$). The findings of the study prove that the protection

motivation factor, that is the threat assessment skills has a significant positive influence on threat coping skills to protect the security of personal data among youths. Therefore, the middle and late youths need to be nurtured with knowledge related to threat assessment to ensure that their data remains protected despite actively interacting and conducting various online transactions.

Keywords: Motivation protection, personal data security, youth

INTRODUCTION

Beginning in 2019, the coronavirus (COVID-19) outbreak has been declared by the World Health Organization (WHO) as a pandemic. The first case in Malaysia was reported by the WHO on 24 January 2020. The implications of this pandemic have changed the entire landscape of universal human life towards adaptation to new norms to continue to survive. The Movement Control Order (MCO) introduced in Malaysia to break the chain of transmission is a catalyst for the rapid use of online service facilities. Following the behaviour of disclosing personal information while conducting transactions or communicating online without vigilance has shown an increase in cases even though the government through the Ministry of Communications and Multimedia Malaysia (MCMC) and its agencies have issued warnings to maintain personal confidentiality.

The spread of COVID-19 has led governments, institutions, and organizations worldwide, including Malaysia, to utilize technology for tracking and data-driven tools to monitor and contain the spread of this pandemic. At the same time, large-scale attacks on privacy and personal data protection have also occurred in dealing with this health crisis (Zwitter & Gstrein, 2020). Nonetheless, in situations like these, there is an urgent requirement to take all necessary actions promptly to prevent this crisis from lingering (Sevastopulo & Johnson, 2020). Following the Movement Control Order (MCO), all governmental bodies and corporate enterprises adopted remote work as a measure to disrupt the transmission chain of the COVID-19 pandemic. At that time, administration and all business transactions are conducted online. According to the Future Jobs Report 2020, 84 percent of jobs in the COVID-19 pandemic era have transitioned

to a digital base to ensure the continuity of operations and services (World Economic Forum, 2020).

Related to complying with the policies of Movement Control Orders (PKP) and social distancing, one of the global governments to maintain the continuity of daily activities is adapting to the new norms by shifting daily activities electronically (Mai & Tick, 2021). A study by Gartner.com found that 88 percent of 548 institutions in the United States encourage or recommend employees to work from home (Arlington, 2020). Hence, data privacy and vulnerabilities of online systems are greatly put to the test (Li & Chong, 2020). The COVID-19 crisis is linked to significantly radical shifts in new norms, creating possibilities for cybercrime and an unprecedented criminal justice system situation (Gil, Llinares, Moneva, Kemp & Castano, 2021; Ribeiro, Burkhardt & Caneppele, 2021).

In Malaysia, the Personal Data Protection Act 2010 (PDPA), also known as Act 709, was formulated with reference to the General Data Protection Regulation (GDPR) pioneered by the European Union (EU). Shared aspects in both legislations involve employee personal details, religious affiliations, relationship information, medical records, financial particulars, payroll registers, work performance, and related data, all of which are considered protected personal information under both acts (Alagaratnam, 2021). The primary purpose for the introduction and enforcement of this act is to regulate the processing of personal data through commercial transactions in order to protect individual's personal information. Commercial transactions, within this context, involve business activities such as trade, insurance, banking, buying and selling, and services. However, there are situations where this act does not apply, such as cases involving credit reporting agencies, non-commercial transactions, personal/family/household matters, federal and state governments, and data processing conducted outside Malaysia. According to the National Bank of Malaysia, common issues related to personal data breaches that lead to financial crimes include fake online investments and various types of fraud such as parcel scams, love scams, Macau scams, and fake internet banking or phishing (National Bank of Malaysia, 2017).

Azul and Madiha (2017) found that uncontrolled sharing of personal information by users on the internet or social media leads to negative impacts such as personal information theft, data breaches, information misuse, and more. It is believed that cyber-crimes are becoming increasingly difficult to handle if social media users lack the awareness to control or select their online personal information sharing. Examples of personal data security threats are identity theft, phishing, fraud, and cyberbullying. Such cases occur after individuals expose their personal information on social media platforms like Twitter, Facebook, LinkedIn, and others (Kumar, Gupta, Rai & Sinha, 2013). In some cases, cybercriminals set up websites to sell fake products and use fake emails, SMS, and social media accounts to trick victims into giving away money or providing personal information (Tressler, 2020). The activity of uploading personal information on social media tends to become one of the threats to users' privacy (Bahri, Carminati & Ferrari, 2018).

A British technology website reported the findings of a study on 47 countries regarding privacy protection and state surveillance assessment based on 15 criteria. The study revealed that Malaysia ranks in the bottom five positions with a score of 2.64 (Bischoff, 2021). The threat to personal data security is identified as a "when" issue rather than an "if" issue, therefore stakeholders need to remain vigilant by taking crucial actions, including developing strategic plans, formulating responses, determining the severity of incidents, and assigning roles to relevant parties (Neubauer, 2022). Moreover, this extraordinary phenomenon highlights that in contemporary times, there has been no catalyst that has presented such extensive opportunities for digital crime in such a short period, other than the COVID-19 pandemic (Kemp, Gil, Moneva, Llinares & Castano, 2021).

LITERATURE REVIEW

Digital penetration

The Global Digital 2021 report indicates that the world's population is 7.83 billion at the beginning of 2021. Based on this figure, the United Nations (UN) has stated that the population is now increasing by 1 percent annually. This signifies a global increase of 80 million people since 2020 (Kemp, 2021). The report also mentions that there are 5.22 billion mobile phone users, which is equivalent to 66.6 percent

of the world's population. These statistics show an increase of 1.8 percent (93 million people) starting from January 2020. Additionally, the report concludes that there are a total of 4.66 billion internet users worldwide as of January 2021, with an increase of 316 million or 7.3 percent since 2020. This means that the global internet penetration rate stands at 59.9 percent. As for social media users, there are 4.20 billion individuals globally, showing an increase of 490 million over the past 12 months. This growth rate is more than 13 percent. These statistics indicate that the number of social media users now represents over 53 percent of the total global population.

In tandem with the global growth of internet usage, the Malaysian government has allocated provisions to enhance digital connectivity and digitization in the budget for the year 2021 (Ministry of Finance Malaysia, 2021). Subsequently, the continuity of this initiative was upheld in the federal budget allocation for the year 2022 (Ministry of Finance Malaysia, 2022). Everyone is using smart digital devices and tools, causing the social system to be fully interconnected as the 'Internet of Things' (IoT) to enhance the quality of life. However, this situation presents a major challenge in terms of the security and privacy of user data (Mehak, 2019). Therefore, it is essential to identify strategies and preferences for understanding issues concerning digital security and technology access to prioritize.

Youth of Malaysia

The Malaysian Youth Policy (MYD) was developed in 2015 as a long-term plan blueprint for the Malaysian youth generation until the year 2035. One of the significant elements articulated in the MYD pertains to the definition of youth age, which encompasses individuals aged 15 to just before reaching 30 years old. The MYD also outlines the challenges that youth are expected to face, enabling the policy to serve as a guiding framework for formulating policies that align with future needs and demands. Beginning in 2006, the Institute for Youth Research Malaysia (IYRES) has developed the Malaysian Youth Index (MYI) as a tool to measure the quality and well-being of Malaysian youth. Currently, the MYI in 2021 indicated that the safety indicator when using the internet under the Media and Digital Citizenship domain was scored at 81.7 and increased to a score of 84.57 in 2022.

The youth demographic constitutes the largest segment in Malaysia. A total of 9.0 million or 31 percent of the entire Malaysian population of 32,584.0 million are at the youth age (Department of Statistics Malaysia 2020). It is of utmost importance to prioritize this group to protect them from or prevent more severe cybercrime issues. According to the Department of Statistics Malaysia, 51.60 percent or 4.64 million are male youths, while 48.40 percent, or 4.36 million are female youths aged between 15 and 30 years old (IYRES 2020). The younger generation holds a crucial role in the nation-building process, as they are an asset for the future generation (Pandian, 2005). It's important to prioritize this group to ensure their prevention of more critical cybersecurity issues.

Youth and Personal Data Security Threats

Malaysia is now facing a personal data security crisis. The Malaysian Cyber Consumer Association (MCCA) expressed concern over the increasing activity in the theft of banking login data or any financial applications and websites and consumers' social sites (Aling, 2020). In addition, Anonymous Malaysia warned that Malaysia's security systems were at a low level and could lead hackers to sell all the leaked information and that more than 46 million telecommunication companies' user data had been hacked (Anon, 2021).

The Malaysian Youth Policy (MYP) (2015-2035) has outlined four major youth challenges by 2035. One of them is challenges in technology and the digital world. Based on these challenges, the Malaysian Internet Users Survey by the Malaysian Communications and Multimedia Commission (MCMC) in 2020 showed that 47.0% of Malaysian Internet users feel safe using the Internet. Meanwhile, their confidence level in their data protection after sharing personal data with the government sector was recorded 50.4%, the non-government sector 40.2% and service providers 40.6%. Coinciding with this scenario, this study was conducted based on the Protection Motivation Theory (PMT) by Ronald W. Rogers (1975). PMT is very powerful in testing fear based on past experiences and is the motivation to change behaviour to comply with a policy by the government (Anderson & Agarwal, 2010; Vance & Pahnla, 2012; Mahbob et al., 2013). This study used two constructs under PMT: threat assessment and threat coping skills. DBM defines the age of Malaysian youth from 15 years to 30 years old. Editing of data by IYRES based on the projected data of the Department of Statistics Malaysia (DOSM, 2020) shows that the youth age group represents 27%

of the total Malaysian population of 33.7 million people. In this regard, this study was adopted and adapted to the Malaysian youth group which is an age group that should be vulnerable to the challenges of today's digital world.

Liang and Xue (2010), found that both threat assessment skills and threat coping skills were important factors for studying computer threat avoidance behaviours. Anyone of us takes precautions to download or update antivirus software to protect their data online and is willing to pay the costs (Tsai, Jiang, Alhabash, LaRose, Rifon & Cotton, 2016). This step is taken because they are aware of the risks of neglecting the security of their data when using an application or website. Furthermore, their own experiences or other people's experiences such as identity theft cases, security of financial information and phishing attacks serve as reminders to safeguard their professional reputation and personal life (Internet User Survey, 2020; Rainie, Kiesler, Kang & Madden, 2013).

Beginning from year of 2020 era, the Pandemic Covid-19 brings new challenges to data protection in this century. Every country uses a digital mechanism to combat a health crisis around the world. In comparison, NHS COVID-19 used in UK, Covid Tracker in Ireland, StopCovid in France, Smittestop in Denmark, Corona Melder in the Netherlands, Immuni in Italy, JianKangBao in China (Wang & Cahill, 2023) and MySejahtera used in Malaysia. In this critical scenario, where personal data is collected by the government and as citizens, we have no option but to say yes to obey the needs of the nation.

They find themselves uncertain between disclosing the information or keeping it to themselves in silence. Throughout the pandemic, generally noticed that the personal information of positive covid-19 patients circulated across social media platforms, without awareness of the legal infringement upon their privacy. Data pertaining to COVID-19 has reportedly been stolen from government servers and sold, according to the Indian Express, which includes name, age, gender, mobile number, address, date, and result of COVID-19 report (Dar & Wani, 2023). While carrying out the operation of personal data in a pandemic including health data, privacy and data protection become critical in their rollout (Brand Equity, 2022).

Learn from personal experiences, enhanced an intuition to individuals as a motivation to protect their personal data, and encourage the development of protective behaviors. Thus, this study aims to examine the factors influencing Malaysian youth to protect their privacy data when communicating or conducting transactions online. This study used two main constructs of protection motivation which is threat assessment and threat coping skills.

METHODOLOGY

The study used a quantitative method using questionnaires conducted online. A total of **535** respondents were randomly selected using a multi-stage random sampling approach. This approach is implemented to ensure that youths from the two study locations, namely Putrajaya and Cyberjaya have homogeneous characteristics with an equal probability of being selected as study subjects. These two locations were selected because they are the locations of the Multimedia Super Corridor (MSC) hub and the smart city. In 2019, the government through MCMC in collaboration with Maxis and Huawei chose this location for the testing of 5G broadband services for free before being expanded throughout Malaysia. This service gives an advantage to the youth in this location to use the wider Internet facilities than the youths in other locations. This study focuses on middle youth (19-24 years old) to late youth (25-30 years old) as the subject of the study considering that they have been in the labor market and using Internet facilities in everyday life.

The simple regression analysis was conducted using the parametric analysis of SPSS software (version 25) to see the effect of the influence of threat assessment skills on threat coping skills. Fundamentally, the main purpose of using regression analysis is to study the relationship between the dependent and independent variables using mathematical formulas (Pallant, 2011; Tabachnick & Fidell, 2013). The three main indicators for reporting the regression relationship for the variables studied are the regression coefficient or the value of r . Followed by the percentage of variants and Beta values as shown in Table 1 to Table 3 below.

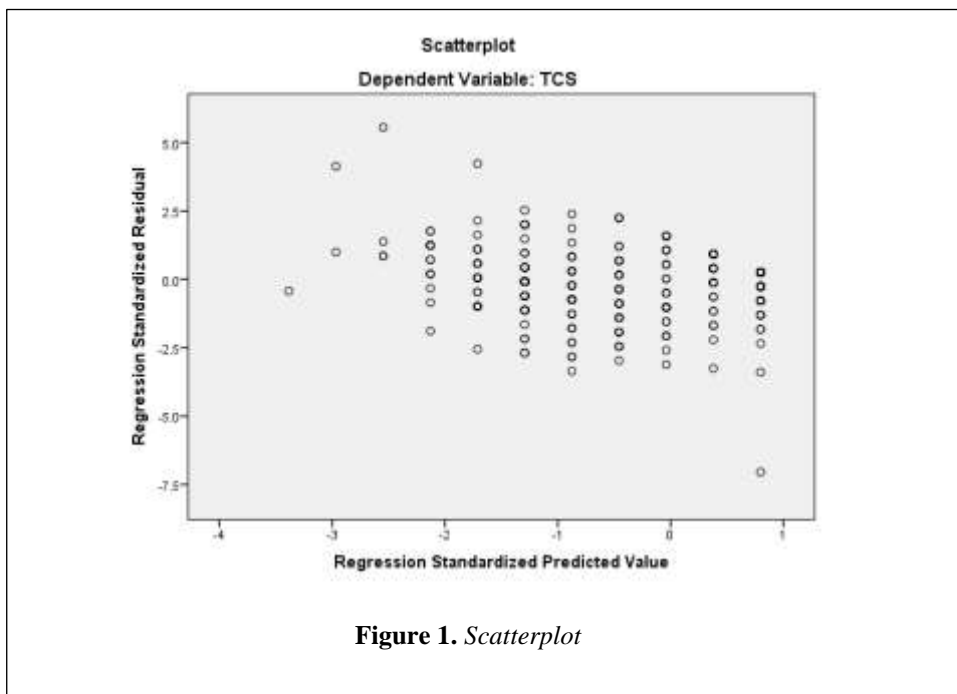
DISCUSSION AND FINDING

The data obtained were analyzed using a simple regression test. This test is a commonly used method to understand the relationship between two independent variables with dependent variables. The formula for this test is as follows:

$$Y = \beta_0 + \beta_1 X_1$$

Y is the threat coping skills (TCS), β_0 is the value of Y, β_1 is the value of the regression coefficient and X_1 is the value of Threat Assessment (TA). Based on the formula, the fit regression coefficient model is $Y = 4.120 + 1.268X_1$. Overall, the value of the regression coefficient is significant ($R^2 = .845$, $F = 1335.428$, $p < .000$). The findings explain that Threat Coping Skills (TCS) were significantly influenced by the Threat Assessment (TA) ($\beta = 1.268$, $p < .000$).

At the initial stage of this test, the accuracy of the model (fit model) can be explained through the scatterplot diagram below. This plot is used in reference to errors or residuals. The plot illustration shows a clustered linear pattern between 0 digits on the x and y axes. Overall, the plot does not show a clear pattern. The findings of this plot illustrate that the model used does not have a clear error.



Model Threat Coping Skill (TCS) and Threat Assessment (TA)

Further, a detailed description is in Table 1 which shows the test on the Threat Coping Skills (TCS) variable with the Threat Assessment skills (TA) variable. It was found that the value of $R^2 = .845$.

Table 1.*Model Summary^b*

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.845^a	.715	.714	1.91741

a. Predictors: (Constant), Threat Assessment

b. Dependent Variable: Threat Coping Skills

Based on the value of the R^2 , it shows the variation value on this variable is .845. This indicates that 84.5% of threat coping skills (DV) could not be described using threat assessment skills (IV). The remaining 15.5% of DV variations cannot be explained using one IV alone. The findings explain that in the context of this study, other factors contribute to threat-coping skills other than threat assessment skills.

Table 2 is an interpretation of the hypothesis developed whether accepted or failed to be accepted. H_1 for this article is that threat assessment skills have a significant relationship with threat coping skills to protect the security of personal data among Malaysian youth. The findings showed that the value $p=.000$ is below the significant value, meaning that H_0 is rejected and H_1 is accepted. It can be concluded that there is a significant relationship between threat assessment skills and threat coping skills to protect the security of youths' data transactions/communications online.

Table 2.
ANOVA^a

Model	Sum of Squares	df	Mean Square	F	Sig.
Regression	4909.658	1	4909.658	1335.428	.000 ^b
Residual	1959.557	533	3.676		
Total	6869.215	534			

a. Dependent Variable: Threat Coping Skills

b. Predictors: (Constant), Threat Assessment

Table 3 describes the direction and relationship between the variables used in this study. The findings show that each significant increase in the value of threat assessment skills will improve the threat coping skills of 1.268 units.

Table 3.
Coefficients^a

Model	Unstandardized Coefficients	Standardized Coefficients	Beta	t	Sig.
	B	Std. Error			
(Constant)	4.120	1.151		3.578	.000
Threat Assessment	1.268	.035	.845	36.544	.000

a. Dependent Variable: Threat Coping Skills

In conclusion, a simple regression test was conducted using the 'Enter' method. The test results showed that the threat assessment skills variables contributed significantly to the threat coping skills, $F=1335.428$, $p < .000$. The Threat assessment skills explained 84.5% of the variation in threat coping skills. The results of the analysis have shown that independent variables contribute to the threat coping skills as a primary predictor ($\beta = 1.268$, $p > .000$).

DISCUSSION, IMPLICATION AND SUGGESTION

The results of the analysis showed that the protection motivation factor, that is the threat assessment skills, has a significant positive level on the threat coping skills to protect the security of personal data among youth. The findings of this study are in line with the essence of protection motivation theory where awareness of the dangers of internet use in daily life will lead to action to assess the threats to its use. The knowledge aspect of the possibility of fraud and theft of personal data is also bringing about a change of vigilant attitude in the evolving digital world. Awareness of personal data security is influenced by the behavioral motivation to safeguard personal data security (Safa, Sookhak, Solms, Furnell, Ghani & Herawan, 2015).

Furthermore, Schaik, Jansen, Onibokun, Camp & Kusev, (2018) proposed that further studies be conducted using the protection motivation theory model as part of preventive measures to address issues of safety and privacy online. This follow-up study is important for better understanding individuals' tendencies to protect themselves from safety hazards and privacy risks related to social media. According to Siponen, Mahmood and Pahlila (2014), there exists a strong inclination to understand the messages and indicators associated with the security of personal data while conducting online activities. This inclination can prompt individuals to take protective measures by initiating alerts and cultivating skills to effectively address these potential threats. Additionally, the study by Boss, Galletta, Lowry, Moody & Polak (2015) discovered that there is a direct influence, such as the feeling of fear of behavioral changes, issuing warnings (Anderson & Agarwal, 2016), and providing alerts for behavior change (Jenkins & Durcikova, 2013).

The significant influence of threat assessment on threat coping skills is highly relevant and consistent with the results of past studies (Rainie et al., 2013; Liang & Xue, 2010), stating that awareness and experience will bring behavioural changes to threat assessments that help counter cyber threats. Therefore, middle and late youths need to be injected with knowledge related to protection motivation to ensure that their data remains protected despite actively interacting or transacting online.

There are six key recommendations from the United Nations (Human Rights Council) regarding personal data collected during the pandemic: (1) Verify compliance with the principles of purpose; (2) Strengthen accountability; (3) Demonstrate transparency; (4) Proactively implement a risk management system; (5) Reinforce a public culture of ethical use of personal data and, (6) Implement a simple and publicly accessible mechanism that allows citizens to verify the use, storage, and deletion of data (United Nation, 2023). The key perspective from this recommendation is the way to empower human rights in the context of personal data protection begins with the individual. This is in line with this study that found each of us especially youngsters to have the skill to protect their personal data

CONCLUSION

In a nutshell, the findings of this study can be used as a reference by the MCMC to continue the campaign strategy to protect personal data security focusing on youths and Malaysians in general. In addition, youth development stakeholders in Malaysia especially MYS through various departments/agencies can conduct various government-wide approach programs to make this effort a success. In addition, further studies use constructs such as behavioral control and self-efficacy to equip youth and Malaysians to avoid the threat of personal data security. This strategic planning is important to help youths prepare and adapt to the digital world environment. Furthermore, the post Covid-19 era teaches us, doing nothing is not an option, and taking an initial step to review computing, information technology, and data systems beneficial in attempting to sustain trusted on organization.

The issue of personal data security has now become increasingly intricate and complex. Despite concerns about the potential misuse of their personal data, individuals continue to pursue the desire to use services that have transitioned from being mere preferences to becoming necessities (Blank, Bolsover & Dubois, 2014). Personal data breaches are frequently linked to human error factors (Hammouchi, Othman Cherqi, Mezzour, Ghogho & ElKoutbi, 2019). Therefore, it is crucial and urgent to enhance individuals' awareness of knowledge that can safeguard the security of their personal data concurrent with the enforcement of cybersecurity policy and procedures (Bell & Liu, 2023). Internet users or netizens must consistently remind themselves that the internet is synonymous with public

space; no personal information can be concealed once individuals upload personal data or images, even on online platforms (Kumar, Gupta, Rai, & Sinha, 2013).

The effectiveness of the PMT model depends on the delivery of persuasive messages in the form of threats or fear appeals aimed at eliciting fear and subsequently motivating individuals to address the threats (Moody, Siponen & Pahnla, 2018). Therefore, employing this theory as an approach is reasonable for use as a campaign strategy to promote efforts towards changing behaviors that protect the security of personal data among Malaysian youths.

ACKNOWLEDGMENT

This work was supported in part by the Institute for Youth Research Malaysia (IYRES), the Ministry of Youth and Sports Malaysia, National University of Malaysia (UKM). The authors would like to thank all team members Centre for Research in Media and Communication (MENTION), Faculty of Social Sciences and Humanity, National University of Malaysia for their direct and indirect contributions.

REFERENCES

- Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimedia empirical examination of home computer user security behavioral intentions. *MIS Quarterly*, 34(3), 613–643.
- Anderson, B. B., Vance, A., Kirwan, C. B., Eargle, D. & Jenkins, J. L. (2016). How users perceive and respond to security messages: a NeuroIS research agenda and empirical study. *European Journal of Information Systems*, 25(4), 364-390.
- Anon (2021, February 3). Malaysia dalam keadaan terkawal daripada ancaman siber. *Bernama*. <https://www.kkmm.gov.my/awam/berita/18573-bernama-03-feb-2021-malaysia-dalam-keadaan-terkawal-daripada-ancaman-siber-ceo-csm>.
- Alagaratnam, S. (2021). Malaysia: Perlindungan data peribadi pekerja diMalaysia - Peraturan perlindungan data am (GDPR) dan Akta Perlindungan Data

Peribadi 2010 (PDPA). *Mondaq*. <https://www.mondaq.com/data-protection/1022286/protection-of-employee39s-personal-data-in-malaysia--general-data-protection-regulation-gdpr-and-personal-data-protection-act-2010-pdpa?type=related>.

Aling, Y. A. (2020). MCCA bimbang kegiatan curi data pengguna media sosial. *HarianMetro*.

<https://www.hmetro.com.my/mutakhir/2020/12/652721/mcca-bimbang-kegiatan-curi-data-pengguna-media-sosial>.

Arlington. (2020). Gartner HR Survey Reveals 88% of Organizations Have Encouraged or Required Employees to Work from Home Due to Coronavirus. <https://www.gartner.com/en/newsroom/press-releases/2020-03-19-gartner-hr-survey-reveals-88%2D%2Dof-organizationshave-e>.

Azul, M. & Madiha, N. (2017). Pengalaman dan kesedaran pengguna dewasa terhadap isu pengawasan di media sosial. *Jurnal Komunikasi: Malaysian Journal of Communication*, 33(1), 502-514.

Bahri, L., Carminati, B. & Ferrari, E. (2018). Decentralized privacy preserving services for online social networks. *Online Social Networks and Media*, 6 (June 2021), 18-25.

Bell, N. & Liu, X. (2023). Level of Cybersecurity Readiness of Small and Medium Nonprofit Organizations (NPOs) During COVID-19. *Journal of Strategic Innovation and Sustainability*, 18(2), 1-11.

Bischoff, P. (2021). Which countries have the worst (and best) cybersecurity? *Comparitech*. <https://www.comparitech.com/blog/vpn-privacy/cybersecurity-by-country/>.

Blank, G., Bolsover, G. & Dubois, E. (2014). A New Privacy Paradox: Age, youth and a theory of privacy on social media. *SSRN Electronic Journal*.

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D. & Polak, P. (2015). What do users have to fear? Using fear appeals to engender threats and fear that motivate protective behaviors in users. *MIS Quarterly*, 39 (4), 837-864.

- Brand Equity. (2022, January 22). Covid-19 related data of thousands of Indians leakedonline.*BrandEquity.com*.<https://brandequity.economictimes.indiatimes.com/news/digital/covid-19-relateddata-of-thousands-of-indians-leakedonline/89059409>.
- Dar, M. A. & Wani, S. A. (2023). COVID-19: Personal Data Protection and Privacy in India. *Asian Bioethics Review*.15, 125–140. <https://doi.org/10.1007/s41649-022-00227-0>.
- Department of Statistics Malaysia (DOSM). (2021). Siaran akhbar statistik utama tenaga buruh di Malaysia, Februari 2021. <https://www.dosm.gov.my/v1/index.php?r=column/pdfPrev&id=UXIFcW1pSnhhZUFSSSTc0RDhnR3V3dz09>.
- GDPR privacy policy. (2019). <https://www.privacypolicies.com/blog/privacy-law-by-country/>.
- Gil, D. B., Llinares, F. M., Moneva, A., Kemp, S. & Castaño, N. D. (2021). Cybercrime and shifts in opportunities during COVID-19: A preliminary analysis in the UK. *European Societies in the Time of the Coronavirus Crisis*, 23(1), 47-59.
- Internet User Survey 2020. (2020). Kementerian Komunikasi dan Multimedia Malaysia. Putrajaya.
- Institute for Youth Research Malaysia (IYRES). (2022). Malaysian Youth Index 2022. Putrajaya. Malaysia.
- Institute for Youth Research Malaysia (IYRES). (2021). Malaysian Youth Index 2021. Putrajaya. Malaysia.
- Malaysian Youth Index 2006. (2006). Institut Penyelidikan Pembangunan Belia Malaysia. Putrajaya: Kementerian Belia dan Sukan Malaysia.
- Hammouchi, H., Othman Cherqi, O., Mezzour, G., Ghogho, M. & ElKoutbi, M. (2019). Digging deeper into data breaches: An exploratory data analysis of hacking breaches over time. *Procedia Computer Science*, 1(151), 1004-1009.

- Institut Penyelidikan Pembangunan Belia Malaysia (IYRES). (2021). Putrajaya. <http://ydata.iyres.gov.my/iyresbankdataV2/www/index.php?r=pub/home/readcontent4&id=134>.
- Jenkins, J. L. & Durcikova, A. (2013). What I shouldn't have done that?: The influence of training and just-in-time reminders on secure behavior. Security and Privacy of Information and IS. Thirty Fourth International Conference on Information Systems, Milan.
- Kemp, S., Gil, D. B., Moneva, A., Llinares, F. M. & Castaño, N. C. (2021). Empty streets, busy internet: A time-series analysis of cybercrime and fraud trends during COVID-19. *Journal of Contemporary Criminal Justice*, 37(4), 480-501.
- Kemp, S. (2021, January 27). Special Report: DIGITAL 2021: The Latest Insights Into The 'State Of Digital'. *We are social*. <https://wearesocial.com/uk/blog/2021/01/digit2021-the-latest-insights-the-state-of-digital/>.
- Kumar, A., Gupta, S. K., Rai, A. K., Sinha, S. (2013). Social networking sites and their security issues. *International Journal of Scientific and Research Publications*, 3(4), 1-5.
- Li, L. L. & Chong, K. Y. (2020). Malaysia: Data privacy in the Covid-19 pandemic. *Mondaq*. <https://www.mondaq.com/data-protection/926938/data-privacy-in-the-covid-19-pandemic>.
- Liang, H., & Xue, Y. (2010). Understanding security behaviours in personal Computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems*, 11(7), 394-413.
- Mai & Tick, A. (2021). Cyber security awareness and behavior of youth in smartphone usage: A comparative study between university students in Hungary and Vietnam. *Acta Polytechnica Hungarica*, 18(8), 67-89.
- Mahbob M. H., Rahim, S. & Idros, W. (2013). Acceptance of social innovation in Malaysia Advocacy and the impact of government transformation programme (GTP). *Journal of Asian Pacific Communication*, 23 (2), 223-238.
- Malaysian Youth Policy 2015-2035. (2015). Ministry of Youth and Sports

Malaysia. Putrajaya. Malaysia.

Mehak. (2019). Cyber crime It's impact on youth. *Indian Journal of Law and Human Behavior*, 5(2), 233-239.

National Security Council (MKN). (2021). *Standard Operasi Prosedur*.
<https://www.mkn.gov.my/web/ms/arkib-sop/>.

Ministry of Finance (MOF). (2021). *Laman Khas Belanjawan 2021*.
<https://belanjawan2021.treasury.gov.my/index.php/ms/galeri/infografik-belanjawan-2021>.

Ministry of Finance (MOF). (2022). *Laman Khas Anggaran Belanjawan 2022*.
https://budget.mof.gov.my/pdf/2022/perbelanjaan/Anggaran_Perbelanjaan_Persekutua_2022.pdf.

Moody, Siponen & Pahlila. 2018. Toward a unified model of information security policy compliance. *MIS Quarterly* 42(1), 285–311.

Neubauer, L. (2022). Cybersecurity for Today's Threats: Make Cybersecurity a Business Discipline. *Gartner*. <https://www.gartner.com/en/webinars/4012614/cybersecurity-for-today-s-threats-make-cybersecurity-a-business-discipline>.

National Bank of Malaysia. (2017). Ringgit. Pelanggaran data peribadi menerusi pembelian dalam talian. *Edisi Oktober (10)*.
<https://www.bnm.gov.my/documents/20124/bb7cb339-914c-bb4b-3725-c91609c1ceda/>.

Pallant J. (2011). *SPSS Survival Manual: A step by step guide to data analysis using SPSS 4th edition*. Allen & Unwin. Australia.

Pandian, A. (2005). Literasi dalam kalangan generasi muda: Perubahan dan cabaran. Prosiding Seminar Penyelidikan Pembangunan Generasi Muda: Realiti Generasi Muda Melangkah Ke hadapan. Fakulti Sains Sosial dan Kemanusiaan, UKM.

Personal Data Protection Act (Act 709). (2010). Ministry of Communication and Multimedia Malaysia. Putrajaya. Malaysia.

- Rainie, L., Kiesler, S., Kang, R., & Madden, M. (2013). Anonymity, privacy, and security online. *Pew Research Centre*.
<http://pewinternet.org/Reports/2013/Anonymity-online.aspx>.
- Ribeiro, S., Burkhardt, C. & Caneppele, S. (2021). Covid-19 crime and criminal justice: Mapping criminological research project around the world. Research Briefs, Series UNILCRIM.(7).https://wp.unil.ch/covidcrimeworkinggroup/files/2021/10/Covid19_Research_Projects_UNIL_30092021-1.pdf.
- Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Psychology*, 91(1), 93–114.
- Safa, N. S., Sookhak, M., Solms, R. V., Furnell, S., Ghani, N. A. & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computer and Security Journal* (53), 65-78.
- Sevastopulo & Johnson, P. J. (2020). G7 countries vow to do ‘whatever is necessary’ to support global economy. *Financ Times*.
<https://www.ft.com/content/571f51e0-67b3-11ea-800d-da70cff6e4d3>.
- Siponen, M., Mahmood, A. & Seppo Pahnla, S. (2014). Employees’ adherence to information security policies: An exploratory field study. *Information & Management*, 51(2), 217–224.
- Schaik, P. V., Jansen, J., Onibokun, J., Camp, J. & Kusev, P. (2018). Security and privacy in online social networking: Risk perceptions and behaviour. *Computers in Human Behavior*, 78, 83-297.
- Tabachnick B. G & Fidell L. S. (2013). Using Multivariate Statistics (4th Edition). HarperCollins. New York.
- Tressler, C. (2020). Coronavirus: Scammers follow the headlines. *Federal Trade Commission*.
<https://consumer.ftc.gov/consumer-alerts/2020/02/coronavirus-scammers-follow-headlines>.
- Tsai, H. S., Jiang, M., Alhabash, S. LaRose, R., Rifon, N. J. & Cotton, S. R. (2016). Understanding Online Safety Behaviors: A Protection

Motivation Theory Perspective. *Computers & Security*, 59(June 2016), 138-150.

United Nation. (2023, March 14). Right to privacy must be safeguarded in post pandemic world: UN expert. *United Nation Human Right Press Release*.
<https://www.ohchr.org/en/press-releases/2023/03/right-privacy-must-be-safeguarded-post-pandemic-world-un-expert>.

Vance A. M. & Pahnla S. (2012). Motivating IS security compliance: Insights From Habit and Protection Motivation Theory, *Information & Management*, 49 (3-4), 190-198.
<https://doi.org/10.1016/j.im.2012.04.002>.

Wang, J. & Cahill, D. (2023). Personal Data Privacy vs Public Interest: Covid-19 Data Gathering Brings a Personal Data Protection Policy Rethink. *Academic Journal of Nawroz University (AJNU)*, 1 (1), 1-12.
<https://doi.org/10.25007/ajnu.v1n1a1940>.

World Health Organisation (WHO). *Covid-19 in Malaysia*.
<https://www.who.int/malaysia/emergencies/covid-19-in-malaysia>.

World Economic Forum. 2020. *The future of jobs report 2020*.
https://www3.weforum.org/docs/WEF_Future_of_Jobs_2020.pdf.

Zwitter, A. & Gstrein, O. J. (2020). Big data, privacy and COVID-19 – learning from humanitarian expertise in data protection. *Journal of International Humanitarian Action*, 5(4), 1-7.