Jurnal Komunikasi:
*Malaysian Journal of Communication*
Jilid 39(1) 2023: 336-352

# Security Threats to Privacy Data of Malaysian Youth's: Online Transaction and Communication

SHARIFFAH MAMAT
*Institute For Youth Research Malaysia (IYRES)*

WAN AMIZAH WAN MAHMUD
ARINA ANIS AZLAN
*Universiti Kebangsaan Malaysia*

ABSTRACT

The new norms during the COVID-19 pandemic contributed to the increased usage of the online medium. The International Labour Organization (ILO) reports that millions of people were forced to stay at home during difficult situations (2020). Both the government and corporate sectors are changing the landscape of their services to online services. Apart from its benefits, the rapid adoption of technology also increases the risk of data breaches among individuals' personal information. This article focuses on the intention factor as a motivation to protect the security of personal data among the youth. A total of 535 respondents in the range of 19 to 30 years old from Putrajaya and Cyberjaya. They are randomly selected using a multistage cluster sampling method. A set of questionnaires were distributed online during the Movement Control Order (MCO) that hit all over the world including Malaysia. To analyse factors affecting the Malaysian youth in protecting the security of personal data the multiple linear regression analysis was applied. This article reports the intention factor has a dominant influence in motivating Malaysian youth to protect the security of their data. Additionally, findings showed that family connection and online banking transactions as the main factors in using online compared to other motives measured in this study. Therefore, Malaysian youths should be given the knowledge and awareness to keep on vigilant and protect their data security. Their motivations need to be nurtured to ensure that Malaysian youth's personal data remain protected even if they are actively interacting online.

**Keywords:** *Intention, threat assessment, coping skills, data privacy, youth, online*.

## INTRODUCTION

2019 was the starting point when the World Health Organization (WHO) announced the pandemic of coronavirus (COVID-19) that had spread throughout the globe (World Health Organization, 2020). Such a health crisis had never occurred in the history of human civilization which caused the world to stall in 2020 (Ahmad, 2022). In its early stages, the outbreak was identified only as an epidemic in Wuhan, China and then unexpectedly spread out rapidly from China to other countries where Malaysia was no exception. On 24th January 2020, WHO reported the precedent case had spread in Malaysia, and the topmost total number of daily cases reported was on 20 August 2021 at 23,564 cases (Ministry of Health Malaysia, 2021). Approaching the year 2022, the daily cases had declined and on January 1st, 2022, 3,386 cases were recorded and cumulatively Covid-19 cases in Malaysia totalled to 2,761,472 (Ministry of Health, 2022).

The implications of this pandemic have changed the landscape of entire human life to adapt to the new norms. The coronavirus catastrophe is accompanied by a new change in norms that is so drastic and triggers opportunities for cybercrime or cyber threat that are unprecedented (Gil, Llinares, Moneva, Kemp & Castano, 2021; Ribeiro, Burkhardt &

E-ISSN: 2289-1528
https://doi.org/10.17576/JKMJC-2023-3901-19

Caneppele, 2021). The outbreak of COVID-19 was a catalyst to opportunities in digital crime in a short period throughout the extraordinary phenomena that occurred in this contemporary era (Kemp, Gil, Moneva, Llinares & Castaño, 2021).

Additionally, the threat of cybercrime is expected to be greater than the COVID-19 pandemic as it can also lead to loss of life, and impact businesses and the country's economic status (Bernama, 2021). Besides affecting public health, the COVID-19 pandemic also disrupted the economic and sociocultural survival of the community (Ali & Malaco, 2022). A study by the London-based Department for Digital, Culture, Media, and Sport confirmed that higher risk levels occurred during the COVID-19 pandemic thus leaving businesses more impacted to handle cyber security measures (Department for Digital, Culture, Media and Sports, 2021).

The COVID-19 pandemic that spread throughout the country has not yet shown a sign of an end and has driven the use of digital technology in daily transactions including business operations (Berger, 2021). According to IBM Security (2021), the average loss involving data intrusion for companies with a larger cloud of USD 5.12 million compared to USD 3.46 million before the pandemic. A magazine focusing on personal data security based in Singapore revealed that on average, the websites of the most influential Fortune 1000 business magazines in the United States have 135 third parties' data requests to enrich business models, build profiles and disclose their customers' information (Barnett, 2022). Like other countries around the world, Malaysia through the National Security Council implemented the Movement Control Order (MCO) to break the precession of COVID-19 transmission (Majlis Keselamatan Negara, 2022). A study by Gartner.com found that 88% of the 548 institutions in the United States encouraged or recommended employees to work from home (Baker, 2020). It is undeniable that changes in the new norm are a catalyst for the rapid use of online service facilities.

The consequences of disclosing personal information while transacting or communicating online without being vigilant have shown an increase in cases even though the government through the Ministry of Communications and Multimedia Malaysia (MCMM) and its agencies have issued warnings to maintain personal confidentiality. The strategy of working from home and online shopping on a large scale around the world as part of the new norm to control the virus from spreading also contributes to the deviation in opportunities for committing crimes online (Hawdon, Parti & Dearden, 2020; Payne, 2020). Various employment in large, medium, or in small scale has started to expand their services and products online including the banking sector. As a result, the banking sector is exposed to the high jeopardy of online transaction security threats. Hence, banking institutions in Malaysia have developed cyber security strategies by establishing cyber security and data protection units in the Department of Digital and Technology as part of their governance. This strategy is undertaken to strengthen and ensure that risk management involving banking activities is well managed to gain the trust of their customers (Bank Negara Malaysia, 2020). The outbreak of the deadly virus has increased digital transformation in the banking and e-commerce sectors as consumers are forced to embrace radical changes to interact with financial institutions or deal with e-commerce (Al-Saadi, 2021; Vasenska, Dimitrov, Davidkova, Krastev, Durana & Paulakiet, 2021).

In Malaysia, the government through the Ministry of Communications and Multimedia Malaysia (MCMM) introduced the Act of 709 which is the Personal Data Protection Act in 2010. The act was purposely developed to allow the handling of personal data in commercial businesses in Malaysia. Commercial transactions in this context involve business activities

such as trade, insurance, banking, sale, and services. However, several situations do not apply to this act involving credit reporting agencies, non-commercial transactions, personal/family/household matters, federal and state governments, and data processed outside Malaysia. According to the Bank Negara Malaysia (2017), Act 709 also entitles individuals to matters such as (1) to be notified of the probability of an organization processing their personal data; (2) to access their own personal data; (3) to correct their own personal data; (4) to revoke consent to process personal data; (5) to avoid processing that may trigger harm or stress and (6) to avoid processing for direct promoting purposes.

A commentary on privacy rights was revealed in the media stating that the 'right of personal privacy of every person in the country is guaranteed by law. Previously, the law of the right to personal privacy was vague. This is because Act 709 was enacted based on 'Common Law' and further reinforced by the debate in the Parliament of Malaysia through the Personal Data Protection Act, 2010 (Act 709) which was enforced in 2013 (Buang, 2020). Despite having strict internet network security it is also seen that cybercriminals had intensified their cyber-attack weapons such as Ransomware which extorted money from victims (Kaspersky, 2021).

## LITERATURE REVIEW OR RESEARCH BACKGROUND

### *Personal Data Security Threats*

Not just Malaysia, but many countries were facing a personal data security crisis. The disclosure of a report claiming that a total of 4 million Malaysian data belonging to the National Registration Department (NRD) were leaked and attempted to be sold online for RM35,000 (Rozlan, 2021). This issue is a concern to various parties as the cyber threat not only threatens the owner of the personal information but also gives the impression that the country's cyber security level is at a dangerous level. The low level of awareness of the basics of internet knowledge contributes to the increase in cases related to online fraud, online disruption, and identity theft (Ahmad & Othman, 2019). The excitement over the advancement and rapid pace of technology that opens borderless spaces for youth has been manipulated by irresponsible parties (Ishak, Ismail, Mat, Kassim, Mamat & Talib, 2016).

A British tech website reported the results of a study on the assessment of privacy protection and national surveillance of 47 countries based on 15 criteria and found that Malaysia was ranked in the bottom five with a score of 2.64 (Bischoff, 2021). The report also revealed that among the criteria which demonstrate privacy vulnerabilities and surveillance of cyber security controls in Malaysia include constitutional and statutory protections, privacy enforcement, and government access to data (Majid & Alizan, 2019). Based on the report, the legal expert recommends that the Malaysian government should adapt to the technologically advanced environment and enforce the limitation of sharing of personal data between agencies that are the cause of violations of the legislation enacted. Also, according to the legal expert, this strategy is important to prove its seriousness and demonstrate its commitment to protecting data security and the privacy of Malaysian citizens. Personal data security threats are described as 'when' not 'if' problems, therefore stakeholders should always be vigilant by taking action to develop a strategy plan, develop a response, determine the severity of incidents, and assign roles to the relevant parties (Neubauer, n.d.). A survey, The Internet User Survey Malaysia 2020 conducted by the Malaysian Communications and Multimedia Commission (MCMC) reported that about 50.4% of Malaysians feel confident and

secure in their data in government keeping compared to service providers (40.6%) and non-governmental organizations (40.2%) during the outbreak.

*Malaysian Youth Landscape*

According to Organisation and Youth Development 2007 (Act 668), the definition for youth in Malaysia is individuals aged 15 to 40 years old as stated in the National Youth Development Policy 1997, Ministry of Youth and Sports Malaysia (MYS). In the context of positive youth development implementation strategy and activity orientation, the focus is given to youths aged 18 to 25 years old. However, the establishment of the Malaysian Youth Policy (MYP) 2015-2035 as a holistic and futuristic blueprint defines youth as individuals aged 15 to 30 years old. This initiative has outlined the goals, strategies, action plans, and implementation to showcase Malaysian youth potential. Adaptation to technology is one of the four challenges outlined in MYP which focuses on the technology of information and communication, digitalisation, new media, and innovation in science and technology.

According to the Jabatan Perangkaan Malaysia (2021a), out of the total population of 32,584.0 million, there were 9,794.7 Malaysians aged 15-30 years. Based on the total, 51.60% or 4.64 million are male youths while a total of 48.40% or 4.36 million are female youths aged between 15 and 30 years (Institute for Youth Research Malaysia, 2020). Further analysis by the Institute for Youth Research Malaysia (IYRES) and referring to Department Statistics of Malaysia (DOSM) data projections show that the youth age group represented 27% of Malaysia's total population of 33.7 million people (Institute for Youth Research Malaysia, 2021).

*Youth and Challenges of the Digital World*

It was recorded that 59.5% of internet users worldwide in January 2021. Based on that number, 92.6 % had accessed the internet using mobile devices (Johnson, 2021). Based on the challenges of the digital world, the Malaysian Youth Policy (MYP) has outlined four key youth challenges by 2035. The key challenges are technology and the digital world. Based on these challenges, a study on Internet Users Survey 2020 by the Malaysia Communications and Multimedia Commission (MCMC, 2020) revealed a total of 47.0% of Internet users in Malaysia felt safe using the Internet network in their daily lives. The study also reported that the five main activities of Malaysians using online platforms are communication at 98.1%, accessing social media at 93.3%, watching videos at 87.3%, communicating by video at 81.1%, and obtaining information at 74.3%. The Global Digital 2021 reported that the world's population is a total of 7.83 million. Based on this figure, the United Nations (UN) states that it is now increasing by 1% per year. It reflects that the total global population has expanded to 80 million people since 2020 (Kemp, 2021). The report also mentioned that mobile phone users of 5.22 billion people is equivalent to 66.6% of the world's population. These statistics showed an increase of 1.8% (93 million people) in early 2020. The report also concluded that worldwide there were a total of 4.66 billion internet users as of January 2021 with a growth of 316 million or 7.3% since 2020. This means that the percentage of global internet penetration recorded a total of 59.9%. Social media users are recorded as 4.20 million people worldwide and keep an increase of 490 million in the last 12 months. The percentage of growth is greater than 13%. These statistics show that the total social media consumption is now equivalent to or more than 53% of the world's population (Kemp, 2021).

This scenario is supported by a survey during the period of the COVID-19 outbreak in Malaysia. The result of the survey showed a significant finding where Malaysian internet users aged 15 years and older increased from 89.6% in 2020 compared to 84.2% in 2019 (Jabatan Perangkaan Malaysia, 2021b). PEW Research Centre revealed most Americans are using Youtube and Facebook besides using Instagram, Snapchat, and Tik Tok, especially teens aged 30 and below (Auxier & Anderson, 2021). In Malaysia, there has been an increase of 6% in social media users in 2021 from 81% in 2020 to 86%. Facebook is ahead of social media followed by Instagram, Facebook Messenger, and LinkedIn (Muller, 2021). The use of mobile device technology often targets youth age groups with the motive of collecting extensive information without providing a link to privacy or access policies for users to know how their data is being processed (Cohen & Yeung, 2015). Additionally, the marketing provider targeted young social media consumers that shared their personal data information based on the information provided when they used it for the first time (Zarouali, Poels, Ponnet & Walrare, 2018). In this regard, individuals become insensitive to the situation as they are currently benefiting from the services, plus the tendency to not take precautions (Chen, Beaudoin & Hong, 2016).

According to Shin (2020), youths are now often referred to as digital natives whereby they are born and grow up in tandem with the rapid pace of digital technology. Most youngsters are very dependent on technology and know nothing about this world without media in their daily activities. The situation is obscured by the facilities that they obtain by sharing personal information. This is caused by an individual's negligence which can lead to a more dangerous cybercrime threat. The current situation shows two main categories of cybercrime identified which involve cyber-dependent crimes such as software hackers, and attack denials, and secondly are crimes such as phishing, identity theft, cyber romance fraud, and online purchase fraud (Wagen & Pieters, 2020).

Yet what is more worrying is excessive information sharing but the slighter effort to protect the security of personal data which contributed to a target becoming a victim of cybercrime (Larose & Rifon, 2007). This situation also illustrated cyber security vulnerabilities. Therefore, it is an obligation to protect the security and privacy of social media users as more users are exposed to the security and privacy risks of online transactions (Schaik, Jansen, Onibokun, Camp & Kusev, 2018). This is because each individual has his own social influence, level of trust, and ability to protect the security of their personal data (Chen, Hammer & Dabbish, 2019).

It is the right of an individual to make decisions about their data security in this borderless world (Lee, Wong & Chang, 2016). Nevertheless, the issue of personal data security is becoming more complicated and complex as individuals concerned about data misuse continue to pursue the desire to use services that are increasingly becoming a necessity (Blank, Bolsover & Dubois, 2014). Hence, this shows how important it is to understand the youngster's behaviours in decision making based on theories related to human behavioural changes.

*The Theory of Planned Behaviour (TPB) and Youth Personal Data Security*

In line with this phenomenon, the study was designed using the TPB founded by Icek Ajzen (1985). One of the variables in TPB is intention. This refers to a situation whereby the stronger an individual has the intention to change the behaviour from negative to positive, the more likely the individual is to change the behaviour as a lifelong process (Ajzen, 1991; Ajzen, 2020).

*Protection Motivation Theory (PMT) and Youth Personal Data Security*

PMT were introduced by Ronald W. Rogers (1975). Two main constructs under PMT used are threat assessment and threat coping skills. Rogers (1983) has reviewed PMT for application in the discipline of public health and safety research. Briefly, PMT is a theory that explains that when a person is provoked by a threat, cognitively the individual evaluates the threat and finds a way to overcome the threat (Menard, Warkentin & Lowry, 2018). The threat assessment process depends on the severity of the threat which will alert the motivation factor to protect themselves from an individual who deals with the situation itself or through the experience of another individual (Cummings, Chuah & Ho, 2018). PMT has proven is very powerful to test fear based on experience and is a motivation to change the behaviour of adhering to a policy by the government (Anderson & Agarwal, 2010; Vance, Siponen & Pahnila, 2012; Mahbob, Sulaiman, Rahim, Jaafar & Sulaiman, 2013). In this regard, the study adapted to a group of Malaysian youth as a subject of the study. This is an age group naturally vulnerable to the challenges of today's digital world. The combination of theories is shown in the diagram below:

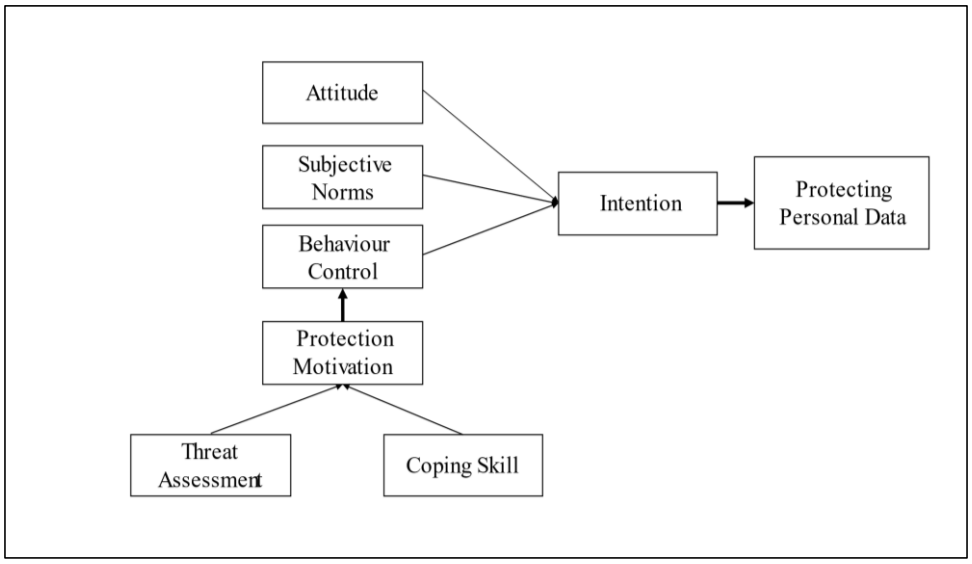


Figure 1: Integration of the TPB and PMT theory

*a. Research Objective*

The aims of this study are to examine the intention factor as a motivation to protect the security of the youths' data when transacting or communicating online. Regarding the objective of this study, the hypothesis of the study is developed as below:

$H_1$: There is a significant relationship between intention as a motivating factor to protect the security of youth privacy data.

The intention in TPB and protection motivation in PMT are widely and commonly used in social phenomena research to change the behaviour of human beings. For example, a study by Cummings, Chuah and Ho (2018) uses the combination of this theory in nanotechnology-based research. Furthermore, a study among young people in Mexico and Colombia on privacy and security in communicating or transacting online by Gastelú, Zanabria and Armenta (2020). Individuals also tend to show a positive attitude if third parties ask for permission to use their data for service marketing purposes (Tsang, Ho & Liang, 2004). The intention is also a complex behaviour to understand (Eri, Islam & Daud, 2011). If the intention factor does not affect a person to change the behaviour, the probability of a behaviour is

influenced by other factors that need to be studied by social science researchers. There are direct influences such as fear of behaviour change (Boss, Galletta, Lowry, Moody & Polak, 2015) and warning (Anderson, Vance, Kirwan, Eargle & Jenkins, 2016) to change the behaviour (Jenkins & Durcikova, 2013). Furthermore, the threat assessment factor influences an individual's behaviour to take more precautions against the spread of COVID-19 information through social media (Allington, Duffy, Wessely, Dhavan & Rubin, 2021). An analysis of followers of the government's social media accounts found that they significantly changed their threat assessment, developed threat coping skills, and enhanced behaviours to protect safety from COVID-19 (Tang, Miller, Zhaou & Warkentin, 2021). The government of Japan also implemented a study to monitor the patterns and media coverage among the young generation during COVID-19 (Lee, 2021). Although an individual has a high confidence level in the response to protect the personal data they shared, sometimes they are not convinced of the actions taken (Boerman, Kruikemeier & Borgesius, 2021).

## METHODOLOGY

This quantitative study used a questionnaire conducted online after obtaining the approval of the university's Ethics Committee. This study involved a total of 535 respondents who are randomly selected by using the multistage random sampling approach. This approach was carried out to ensure that youths from two study locations namely, Putrajaya and Cyberjaya have homogeneous characteristics with equivalent chances of being chosen as the sample of the study. This study focuses on middle youth (19-24 years old) up to the end youth (25-30 years old). The subjects of this study were considered a part of that labor market and had access to Internet facilities in their daily life routine. These two locations were selected based on their location as the Multimedia Super Corridor (MSC) hub and the smart city. In 2019, the government through MCMM in collaboration with Maxis and Huawei selected this location for the testing of free 5G broadband services before being expanded throughout Malaysia. This service gives the advantage to youths in these locations using the Internet facilities more widely than youths in other locations.

The SPSS 25.0 software was applied to analyse multiple regression procedures. This analysis was made to identify the effect of the influence of intention on threat assessment skills and threat coping skills. The purpose of using regression analysis is to study the correlation between dependent and independent variables using mathematical formulas (Pallant, 2011; Tabachnick & Fidell, 2013). The main indicators for reporting the regression relationship of the variables studied are regression coefficient ($R^2$), variant, and Beta value as detailed in the results sections.

## RESULTS AND DISCUSSION

Table 1 shows the profile of the demographic respondents by locality, gender, category of age, ethnicity, and employment status. The findings showed that 282 (52.7%) are respondents from Putrajaya and 253 (47.3%) are from Cyberjaya. Based on gender, 272 (50.8%) are male and 263 (49.2%) are female. The percentage shows no significant difference between gender. Meanwhile, 308 (57.6%) are middle youth aged 19 to 24 years old, and 227 (42.4%) are the end youth aged 25 to 30 years old. A total of 352 (65.7%) are Malay respondents, followed by Indians at 100 (18.8%) and 83 (15.5%) Chinese. The status profile of employment showed that a total of 337 (63.0%) are employed, 165 (30.8%) are studying, and 33 (6.2%) are not employed.

Table 1: Demographic profile

| Profile (n=535) | Description | Frequency | Percentage (%) |
|---|---|---|---|
| Location | Putrajaya | 282 | 52.7 |
| | Cyberjaya | 253 | 47.3 |
| Gender | Male | 272 | 50.8 |
| | Female | 263 | 49.2 |
| Age Category | Middle Youth | 308 | 57.6 |
| | End Youth | 227 | 42.4 |
| Ethnic | Malay | 352 | 65.7 |
| | Chinese | 83 | 15.5 |
| | Indian | 100 | 18.8 |
| Employment Status | Working | 337 | 63.0 |
| | Not Working | 33 | 6.2 |
| | Studying | 165 | 30.8 |

Table 2 shows the motive of the study respondents to use the facilities online. The findings showed that motives related to family/friends and using online banking services showed the highest percentage of 512 (95.7%) and 499 (93.3%) respectively. The trend of online purchasing or shopping recorded 442 (82.6%). Meanwhile, the lowest percentage of 204 (38.1%) are playing games online.

Table 2: Motives for using online services

| Motive (n=535) | Frequency | Percentage (%) |
|---|---|---|
| Connect with family/friends | 512 | 95.7 |
| Online banking | 499 | 93.3 |
| Online shopping | 442 | 82.6 |
| Obtain study information | 290 | 54.2 |
| Obtain job information | 264 | 49.3 |
| Finding new contacts | 222 | 41.5 |
| Online gaming | 204 | 38.1 |

Table 3 shows the analysis of the Threat Coping Skills (TCS) variable with the Threat Assessment Skill (TAS) variable against Intention. The analysis shows the value of $R^2$=.559. Followed by the Durbin-Watson value of 1.902 which indicates that the value meets the weighted value between 0 and 4. The Durbin-Watson value obtained explains that the correlation between residuals is acceptable for further analysis purposes.

Table 3: Summary of model

| Model | R | R Square | Adjusted R Square | SD of the estimation | Durbin-Watson |
|---|---|---|---|---|---|
| 1 | .747[a] | .559 | .557 | 1.18920 | 1.902 |

a. Predictors: (Constant), Coping Skill, Threat Assessment
b. Dependent Variable: Intention

Based on the $R^2$ result, the value of the variation is 55.9%. This suggests that 55.9% of the intent factor (DV) can be explained by threat coping skill variables (IV) and threat assessment skills (IV). The remaining 44.1% of the DV variation cannot be described using these two IVs alone. These findings explain there are other factors that contribute to the intention of changing from negative to positive behaviour which is not covered in this study.

Table 4 refers to the Anova value in the analysis performed. The findings show that $H_1$ was accepted at significant values (F=336.683, p = 0.00b). These findings explain that intention has a significant connection to threat-coping skills and threat-assessment skills. In detail, this data shows that the intention factor influences the behaviour of Malaysian youth in assessing threats and overcoming threats to protect their personal data security.

Table 4: ANOVA[a] result

| Model 1 | Sum of Squares | df | Mean Square | F | Sig. |
|---|---|---|---|---|---|
| Regression | 952.274 | 2 | 476.137 | 336.683 | .000[b] |
| Residual | 752.354 | 532 | 1.414 | | |
| Total | 1704.628 | 534 | | | |

a. Dependent Variable: Intention
b. Predictors: (Constant), Coping Skill, Threat Assessment

Table 5 shows the factors that contribute more to the intention factor to transform the behaviour. The findings showed that the threat coping skills recorded a value of β = .412 compared to the threat assessment skill of β= .366 although both variables were significant p < .001. These findings clearly show that threat-coping skills are a unique contributor more influential than the skill of assessing threats to the Malaysian youth's intention to protect their personal data security.

Table 5: Coefficients result

| Model 1 | Unstandardized B | Standardized Std. Error | Standardized Coefficients Beta | t | Sig. |
|---|---|---|---|---|---|
| Constant | 1.037 | .723 | | 1.436 | .152 |
| Threat Assessment | .274 | .040 | .366 | 6.792 | .000 |
| Coping Skills | .205 | .027 | .412 | 7.634 | .000 |

a. Dependent Variable: Intention

## IMPLICATION

Overall, the study focuses on the security factors of personal data of Malaysian youth aged 19 to 30 years old by applying two theories, namely TPB and PMT. TPB is used as a basis and PMT is combined to improve TPB. The use of these two theories is based on the characteristics of the equation (Milne, Sheeran & Orbell, 2000) which makes these two theories suitable for integration (Pang, Tan & Lau, 2021). Various social science studies have used these two theories simultaneously. A Comparative study between TPB and PMT confirms that TPB is the most significant theory in studying the main constructs of attitudes, subjective norms, and self-efficacy toward the security system policy of internet users compared to PMT (Nasir, Arshah & Hamid, 2018). The researchers also recommended further studies be carried out by various parties based on their findings. This combination of theories has been widely studied in various research subjects across the research field disciplines. Grimes and Marquardson (2019) combined TPB and PMT theories to study the quality of systems to evoke positive social norms, lower threat assessments, improve coping assessments, and influence safer behavioural intentions. The result of this study also explained to the stakeholders the crucial importance of protecting the security of the citizen's personal data in the challenges and adaptation of today's technological rapidity. According to Saizan and Singh (2018),

policymakers need to use input on research results to increase cyber security awareness and, at the same time, lower the statistics of cybercrime cases.

Empirically, it has been confirmed that behavioural change is the key to protecting the security of a youth's data. The youth generation or synonyms as the generation of millennials, echo boomers, boomlets, nexters, generation Y, Nintendo generation, or digital generation are described as sociable, open-minded, and well-informed in the digital world (Raines, 2003). They grew up in a rapidly digital world environment and did not take privacy and security seriously when conducting online dealings. However, it does not mean that they do not care about the personal data that they share online (Daisyme, 2015). Youths are concerned about maintaining the privacy of their data and recommend online service providers provide a more secure additional space to ask questions or open a dialogue on internet security (Das, Cheung, Nebeker, Bietz & Bloss, 2018). A high level of literacy on the security of personal data has significantly contributed to lower levels of privacy concerns (Mekovec & Vrcek, 2020). However, the viewpoint that attracts worry which leads to changes in behaviour is a more effective strategy for protecting the security of an individual's data (Luthfia, Triputra & Hendriyani, 2020). It is acknowledged that the effectiveness of the PMT model depends on the delivery of an appeal-based message in the form of threats or fears aimed at arousing fear and then encouraging them to cope with threats (Moody, Siponen & Pahnila, 2018). Sometimes actions or punishments imposed on the perpetrators of digital crimes also warn other individuals to fear facing the same punishment. The fear factor is capable of being a catalyst toward a more positive behaviour change.

The findings of this study recommend that the decision-makers strengthen the enforcement of Act 709 to protect the rights and interests of all youths in Malaysia who are affected after being victims of cyber threats. Cyber experts must create a more secure user access method (Singh & Singh, 2019) despite being aware that policymakers and stakeholders face significant challenges in enforcing existing laws (Pitchan, Mahmud, Sannussi & Salman, 2015). The determination in enforcing the Personal Data Protection Act (PDPA) or Act 709 gives confidence that the government is positioning a priority on achieving the main objective of the implementation of this act which is to regulate the processing of personal data through commercial transactions. Globally, the General Data Protection Regulation (GDPR) is used as a fundamental for the formation of acts and policies to protect the security of the personal data of its citizens. The similarities between GDPR and PDPA include employees' personal information, religious beliefs, contact information, medical, and financial data, payroll, work performance, and so on (Alagaratnam, 2021). In order to ensure that the rules remain relevant, changes according to the current rules should be implemented. For example, the three global business landscapes that have required changes since the GDPR was implemented in 2018 are (1) privacy and the protection of personal data is now more important than ever to protect business data not only in Europe but around the world; (2) thoroughness and detail where breaches of the GDPR are frequent and considered common and (3) the 'encryption' element needs to be enhanced to ensure the security of personal data is preserved and reduce concerns of data breaches (Lechner, 2020).

In dealing with the big data industry to achieve the goals of the Shared Prosperity Vision 2030 (WKB2030), the provision of security systems needs to be emphasized by industry players. The cryptographic technique using the big data industry-based system is identified as a tool to protect personal data stored, processed, shared, or accessed by non-authority (Fraga-Lamas et al., 2016). The current communication technology uses methods to control access by avoiding dubious data violations. The process to ensure the accurate use of certain

information according to the established basis also plays a role in ensuring that the security system of data is not compromised (Sen, 2014).

In addition, the findings of motives using the internet supported the previous study. They claim that it was important to know the motives for internet use in studies related to the issue of protecting the security of users' personal data (Luthfia, Triputra & Hendriyani, 2020).

## RECOMMENDATION AND CONCLUSION

This study revealed it is important to educate Malaysian youth to control their behaviour by practicing a more positive and active daily lifestyle. It is undeniable that digital technology makes it easier for users. However, it has an impact on social relationships between families and communities (Quaglio & Millar, 2000). People tend to limit themselves to some things valuable to be enjoyed such as the quality of social relationships. The more people are busy getting connected online but disconnected from the people surrounding them, the more value is missing. Thus, quality and well-being can be achieved provided that individuals choose to change behaviour towards more positive either virtually or in the real world.

## ACKNOWLEDGEMENT

The study was conducted among Malaysian youths aged 19 to 30 years old only at two main locations, namely Putrajaya and Cyberjaya. In this regard, it is recommended that this study be extended to Malaysians aged a minimum of 15 years and above by involving data collection throughout Malaysia. This implementation is important to ensure that the challenges of the digital world and the preparation of society 5.0 can be well adapted by various ages. It is undeniable that conquering proficiency in digital literacy guarantees the protection of personal information for both youths and Malaysians. The peace of soul and mind in every Malaysian is essential towards achieving the goal of a sustainable country characterized by Madani Malaysia one day.

## BIODATA

*Shariffah Mamat* is a Doctor of Philosophy (PhD) student at the Media and Communications Centre (MENTION), Faculty of Social Sciences and Humanities (FSSK), National University of Malaysia (UKM). She is also the Chief Executive of Research at the Institute for Youth Research Malaysia (IYRES), Ministry of Youth and Sports Malaysia (KBS) from 2005 to date. Her research more in media and positive youth development-related areas. Email: shariffah@iyres.gov.my

*Assoc. Prof. Dr. Wan Amizah Wan Mahmud* is a Senior Lecturer and Head of the Media Communication Programme at the MENTION, FSSK, UKM. She has been with Sistem Televisyen Malaysia Berhad (TV3), Akademi TV3, Malaysian Institute of Integrative Media (MIIM), Institut Translation Negara Malaysia Berhad (ITNM) and Messrs Sri Ram & Co. She was also appointed to the Film Appeal Committee under the Film Control Division of the Ministry of Home Affairs in 2010. Email: wan_amizah@ukm.edu.my

*Dr. Arina Anis Azlan* is an academician at the MENTION, FSSK, National University of Malaysia (UKM). Her area of expertise is concentrated in the field of health communication and information management. She also frequently used as a consultant to conduct research by the government as well as agencies and the corporate sector. Email: arina@ukm.edu.my

REFERENCES

Ahmad, N. A., & Othman, N. (2019). Information Privacy Awareness Among Young Generation in Malaysia. *Journal of Science, Technology and Innovation Policy (JoSTIP), 6*(2), 1-10.

Ahmad, N. (2022). Dear free Malaysia Today - Your words matter: COVID-19 and its subtle rhetoric. *SEARCH Journal of Media and Communication Research, 14*(1), 19-32.

Ajzen, I. (1985). From intention to action: A theory of planned behaviour. In Kuhl J. & Beckman J. (Eds.), *Action control: From cognition to behaviour* (pp. 11–39). Springer.

Ajzen, I. (1991). The theory of planned behaviour. *Organizational Behaviour and Human Decision Processes, 50*(2), 179-211. https://doi.org/10.1016/0749-5978(91)90020-T

Ajzen, I. (2020). The theory of planned behavior: Frequently asked questions. *Human Behavior and Emerging Technologies, 2*(4), 314-324. https://doi.org/10.1002/hbe2.195

Alagaratnam, S. (2021, January 6). Malaysia: Perlindungan data peribadi pekerja di Malaysia - 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

Al-Saadi, N. (2021). The impact of COVID-19 on banks in the European Union. *Riwqs*, *9*(102). https://www.academia.edu/52453379/The_Impact_of_the_COVID_19_on_banks_in_the_European_Union

Ali, H. M., & Malaco, O. H. (2022). Public health intervention: Exploring crisis communication elements in media reports on COVID-19 in Bangladesh. *SEARCH Journal of Media and Communication Research, 14*(1), 33-48.

Allington, D., Duffy, B., Wessely, S., Dhavan, N., & Rubin, J. (2021). Health-protective behaviour, social media usage, and conspiracy belief during the COVID-19 public health emergency. *Psychological Medicine, 51*(10), 1763-1769.

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. https://doi.org/f82s55

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. *MIS Quarterly, 34*(3), 613-643. https://doi.org/10.2307/25750694

Auxier, B., & Anderson M. (2021, April 7). *Social media use in 2021*. *PEW Research Centre.* https://www.pewresearch.org/internet/2021/04/07/social-media-use-in-2021

Baker, M. (2020, March 19). Gartner HR survey reveals 88% of organizations have encouraged or required employees to work from home due to Coronavirus. *Gartner.* https://www.gartner.com/en/newsroom/press-releases/2020-03-19-gartner-hr-survey-reveals-88--of-organizations-have-e

*Bank Negara Malaysia (BNM)*. (2017). Appendix 3: Personal data protection notice. https://www.bnm.gov.my/documents/20124/2493527/edu_Appendix+3.pdf

*Bank Negara Malaysia (BNM)*. (2020). Risk management in technology (RMiT). https://www.bnm.gov.my/documents/20124/963937/Risk+Management+in+Technology+(RMiT).pdf/810b088e-6f4f-aa35-b603-1208ace33619?t=1592866162078

Barnett, J. (2022, March 22). How can you control what you cannot see? Managing control over customer data. *CPO Magazine.* https://www.cpomagazine.com/data-protection/how-can-you-control-what-you-cannot-see-managing-control-over-customer-data/

*Bernama*. (2021, February 4). Malaysia dalam keadaan terkawal daripada ancaman siber. https://www.bernama.com/bm//news.php?id=1928266

Berger, R. (2021). *Cyber security and data privacy: Key considerations for policymakers*. Huawei. https://www-file.huawei.com/-/media/corporate/Local-site/ca/images/2021/cyber-security-and-data-privacy_en.pdf

Bischoff, P. (2021, September 26 ). Which countries have the worst (and best) cybersecurity? *Compari Tech.* https://www.comparitech.com/blog/vpn-privacy/cybersecurity-by-country

Blank, G., Bolsover, G., & Dubois, E. (2014). A new privacy paradox: *Young People and Privacy on Social Network Sites.* Prepared for the Annual Meeting of the American Sociological Association, 17 August 2014, San Francisco, California. https://doi.org/gf5p65

Buang, S. (2020, November 29). Selamatkan data pengguna MySejahtera? *Sinar Harian*. https://www.sinarharian.com.my/article/112441/khas/pendapat/selamatkah-data-pengguna-mysejahtera

Boerman, S. C., Kruikemeier, S., & Borgesius, F. J. Z. (2021). Exploring Motivations for Online Privacy Protection Behavior: Insights from Panel Data. *Communication Research, 48*(7), 953-977. https://doi.org/10.1177/0093650218800915

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.

Chen, H., Beaudoin, C. E., & Hong, T. (2016). Protecting oneself online: The effects of negative privacy experiences on privacy protective behaviors. *Journalism and Mass Media Quarterly*, *93*(2), 409–429. https://doi.org/10.1177/1077699016640224

Chen, T., Hammer, J., & Dabbish, L. (2019). *Self-efficacy-based game design to encourage security behavior online* (Conference paper). Paper presented at CHI Conference on Human Factors in Computing Systems Extended Abstracts (CHI'19 Extended Abstracts), pp. 1-6. https://doi.org/10.1145/3290607.3312935

Cohen, K., & Yeung, C. (2015). Kids apps disclosure revisited. *Federal Trade Commission*. https://www.ftc.gov/news-events/blogs/business-blog/2015/09/kids-apps-disclosures-revisited

Cummings, C. L., Chuah, A. S. F., & Ho, S. S. (2018). Protection motivation and communication through nanofood labels: Improving predictive capabilities of attitudes and purchase intentions toward nanofoods. *Science, Technology, & Human Values*, *43*(5), 888–916.

Daisyme, P. (2015, December 24). Why millennials don't worry that much about online security. *Entrepreneur*. https://www.entrepreneur.com/science-technology/why-millennials-dont-worry-that-much-about-online-security/254121

Das, G., Cheung, C., Nebeker, C., Bietz, M., & Bloss, C. (2018). Privacy policies for apps targeted toward youth: Descriptive analysis of readability. *JMIR Mhealth Uhealth*, *6*(1), e3. http://doi.org/10.2196/mhealth.7626

Department for Digital, Culture, Media and Sport. (2021). *Cyber security breaches survey 2021 - PDF Version.* Ipsos MORI. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021

Eri, Y., Islam, M. A., & Daud, K. A. K. (2011). Factors that influence customers buying intention on shopping online. *International Journal of Marketing Studies, 3*(1), 128-139. https://doi.org/10.5539/ijms.v3n1p128

Fraga-Lamas, P., Fernández-Caramés, T. M., Suárez-Albela, M., Castedo, L. & González-López, M. (2016). A review on internet of things for defense and public safety. *Sensors, 16*(10), 1644. https://doi.org/10.3390/s16101644

Gastelú, C. A. T., Zanabria, L. F. M., & Armenta, J. A. (2020). Attitude of Latin American youth towards online security and privacy (Conference paper). Paper presented at 2020 X International Conference on Virtual Campus (JICV), 03-05 December 2020. Tetouan, Morocco. https://doi.org/10.1109/JICV51605.2020.9375820

Gil, D. B., Llinares, F. M., Moneva, A., Kemp, S., & Castano, N. D. (2021). Cybercrime and shifts in opportunities during COVID-19: A preliminary analysis in the UK. *European Societies*, *23*(1), 547-559. https://doi.org/10.1080/14616696.2020.1804973

Grimes, M., & Marquardson, J. (2019). Quality matters: Evoking subjective norms and coping appraisals by system design to increase security intentions. *Decision Support Systems*, *119*, 23-34. https://doi.org/10.1016/j.dss.2019.02.010

Hawdon, J., Parti, K., & Dearden, T. E. (2020). Cybercrime in America amid COVID-19: The Initial Results from a Natural Experiment. *American Journal of Criminal Justice, 45,* 546-562. https://doi.org/10.1007/s12103-020-09534-4

*IBM Security.* (2021). Cost of a data breach: A view from the cloud 2021. https://www.ibm.com/downloads/cas/JDALZGKJ

Institute for Youth Research Malaysia (IYRES). (2021). Statistik populasi penduduk & penduduk belia mengikut kategori umur, jantina, etnik, daerah & negeri di Malaysia bagi tahun 2015-2021. *Malaysia Youth Data Bank System.* https://ydata.iyres.gov.my/iyresbankdataV2/www/index.php?r=pub/home/readcontent4&id=134

*International Labour Organisation* (ILO). (2020). COVID-19 and the media and culture sector. https://www.ilo.org/wcmsp5/groups/public/---ed_dialogue/---sector/documents/briefingnote/wcms_750548.pdf

Ishak, M. S., Ismail, A., Mat, B., Kassim, A., Mamat, S., & Talib, N. (2016). The influence of television programs on the social development of youth. *Malaysian Journal of Youth Studies*, 15(9), 29-44.

*Jabatan Perangkaan Malaysia* (DOSM). (2021a). Siaran akhbar statistik utama tenaga buruh di Malaysia, Februari 2021. https://www.dosm.gov.my/v1/index.php?r=column/pdfPrev&id=UXlFcW1pSnhhZUFSSTc0RDhnR3V3dz09

*Jabatan Perangkaan Malaysia* (DOSM). (2021b). Kenyataan media penggunaan dan capaian ICT oleh individu dan isi rumah 2020. https://www.dosm.gov.my/v1/uploads/files/5_Gallery/2_Media/4_Stats%40media/4-Press_Statement/2021/20210412-Kenyataan_Media-Penggunaan_dan_Capaian_ICT_oleh_Individu_dan_Isi_Rumah_2020.pdf

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. *ICIS 2013 Proceedings*, 7. https://aisel.aisnet.org/icis2013/proceedings/SecurityOfIS/7

Johnson J. (2021). Digital population worldwide. *Statista.* https://www.statista.com/statistics/617136/digital-population-worldwide

*Kaspersky*. (2021, Dec 15). How GDPR changed the world, and privacy regulation's future. https://kfp.kaspersky.com/news/how-gdpr-changed-the-world-and-privacy-regulations-future

Kemp, S., Gil, B. D., Moneva, A., Llinares, F. M., & Castaño, N. D. (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. https://doi.org/gmzdz9

Kemp, S. (2021, January 27). Digital 2021: Global overview report. *Data Reportal.* https://datareportal.com/reports/digital-2021-global-overview-report

Larose, R., & Rifon, N. J. (2007). Promoting i-safety: Effects of privacy warnings and privacy seals on risks assessment and online privacy behavior. *The Journal of Consumers Affairs, 41*(1), 127-149. https://www.jstor.org/stable/23860017

Lechner, P. (2020, July 7). GDPR: Three ways the world has changed in privacy law's first two years. *CPO Magazine.* https://cpomagazine.com/data-protection/gdpr-three-ways-the-world-has-changed-in-the-privacy-laws-first-two-years/

Lee, H., Wong, S. F., & Chang, L. Y. (2016). Confirming the effect of demographic characteristics on information privacy concerns. *The 20th Pacific Asia Conference on Information Systems (PACIS 2016)*, 70. https://aisel.aisnet.org/pacis2016/70

Lee, J. (2021). Responses to media coverage of the COVID-19 pandemic and information behaviour in the Japanese context. *SEARCH Journal of Media and Communication,* 13(1), 111-126.

Luthfia, A., Triputra, P., & Hendriyani. (2020). The impact of internet motive and access on the opportunities and risks of teenager internet users in Indonesia. *Solid State Technology, 63*(4), 981-989.

Majid, A., & Alizan, T. A. T. (2019). Data protection - Malaysia's World Ranking. *Mondaq*. https://www.mondaq.com/data-protection/867540/data-protection-malaysia39s-world-ranking

*Majlis Keselamatan Negara* (MKN). (2022). SOP pelan pemulihan negara (PPN). https://www.mkn.gov.my/web/ms/sop-perintah-kawalan-pergerakan/

Mahbob M. H., Sulaiman, W. I. W., Rahim, S. A., Jaafar, W. A. W., & Sulaiman, W. S. 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. https://doi.org/10.1075/japc.23.2.04mah

Malaysian Communications and Multimedia Commission (MCMC). (2020). Internet users survey 2020. https://www.mcmc.gov.my/en/resources/statistics/internet-users-survey#

Mekovec, R., & Vrček, N. (2020). Factors that influence internet users privacy perception. *Proceedings of the ITI 2011, 33rd International Conference on Information Technology Interfaces*, 27-30 June 2011 (pp. 227-232). Cavtat, Croatia.

Menard, P., Warkentin, M., & Lowry, P. B. (2018). The impact of collectivism and psychological ownership on protection motivation: A cross-cultural examination. *Computers & Security*, *75*(June), 147-166. https://doi.org/10.1016/j.cose.2018.01.020

Milne, S., Sheeran, P., & Orbell, S. (2000). Prediction and intervention in health-related behavior: A meta-analytic review of protection motivation theory. *Journal Application Social Psychology*, *30*(1), 106-143. https://doi.org/cdbqcf

Ministry of Health Malaysia (MOH). (2021, August 20). Situasi terkini COVID-19 di Malaysia 20 OGOS 2021. https://covid-19.moh.gov.my/terkini/2021/08/situasi-terkini-covid-19-di-malaysia-20082021

Ministry of Health Malaysia (MOH). (2022, January 2). Situasi terkini COVID-19 di Malaysia 01 JAN 2022. *Covid-19 Malaysia*. https://covid-19.moh.gov.my/terkini/2022/01/situasi-terkini-covid-19-di-malaysia-01012022

*Ministry of Youth and Sports Malaysia*. (1997). National Youth Development Policy 1997.

*Ministry of Youth and Sports Malaysia*. (2007). Youth Association and Youth Development Act. (Act 668).

*Ministry of Youth and Sports Malaysia*. (2015). Malaysian Youth Policy 2015-2035.

Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a unified model of information security policy compliance. *MIS Quarterly*, *42*(1), 285-311. https://doi.org/gdsh6z

Muller, J. (2021). Social media users as a percentage of the total population in Malaysia 2021. *Statista.*

Nasir, A., Arshah, R. A., & Hamid, M. R. A. (2018). The significance of main constructs of theory of planned behavior in recent information security policy compliance behavior study: A comparison among top three behavioral theories. *International Journal of Engineering & Technology*, *7*(2.29), 737-741. https://doi.org/j4gc

Neubauer, L. (n.d). Cybersecurity series: Make cybersecurity essential to the business. *Gartner*. https://www.gartner.com/en/webinar/451821/1064701

Pallant, J. (2011). SPSS survival manual: A step by step guide to data analysis using SPSS. (4th ed.). Allen & Unwin. Australia.

Pang, S. M., Tan, B. C., & Lau, T. C. (2021). Antecedents of consumers' purchase intention towards organic food: Integration of theory of planned behavior and protection motivation theory. *Sustainability*, 13(9), 5218. https://doi.org/10.3390/su13095218

Parliament of Malaysia. (2010). Personal Data Protection Act (PDPA) 2010 (Act 709). *Department of Personal Data Protection*. https://www.pdp.gov.my/jpdpv2/laws-of-malaysia-pdpa/personal-data-protection-act-2010/?lang=en

Payne, B. K. (2020). Criminals work from home during pandemics too: A public health approach to respond to fraud and crimes against those 50 and above. *American Journal of Criminal Justice*, *45*(4), 563-577.

Pitchan, M. A., Mahmud, W. A. W., Sannussi, S. N., & Salman, A. (2015). Control and freedom of the Internet: Challenges faced by the government. *Journal of Asian Pacific Communication, 25*(2), 243-252.

Quaglio, G., & Millar, S. (2020). Potentially negative effects of internet use. *European Parliament STOA*. https://www.europarl.europa.eu/stoa/en/document/EPRS_IDA(2020)641540

Raines, C. (2003). *Connecting generations: The sourcebook for a new workplace.* Boston, MA: Crisp Learning.

Ribeiro, S., Burkhardt, C., & Caneppele, S. (2021). *Covid-19 crime and criminal justice: Mapping criminological research project around the world. Research Briefs* (Series UNILCRIM, Université de Lausanne, Switzerland). Serval. https://serval.unil.ch/en/notice/serval:BIB_8D794DDA3C3D

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Psychology, 91*(1), 93-114.

Rogers, R. W. (1983). Attitude change and information integration in fear appeals. *Psychological Reports, 56*(1), 179–182. https://doi.org/10.2466/pr0.1985.56.1.179

Rozlan, N. I. (2021, September 29). Data empat juta rakyat Malaysia dalam bahaya. *Sinar Harian.* https://www.sinarharian.com.my/article/164055/berita/nasional/data-empat-juta-rakyat-malaysia-dalam-bahaya

Saizan, Z., & Singh, D. (2018). Cyber security awareness among social media users: A case study in German-Malaysian Institute (GMI). *Asia-Pacific Journal of Information Technology and Multimedia*, *7*(2), 111-127.

Schaik, P. V., Jansen, J., Onibokun, J., Camp, J., & Kusev, P. (2018). Security and privacy in online social networking: Risk perceptions and precautionary behaviour. *Computers in Human Behavior, 78,* 283-297. https://doi.org/10.1016/j.chb.2017.10.007

Sen, J. (2014). Security and privacy issues in cloud computing. In A. Ruiz-Martinez, R. Marin-Lopez, & F. Pereniguez-Garcia (Eds.), *Architectures and protocols for secure information technology infrastructures* (pp. 1-45). IGI Global. https://doi.org/j4gf

Shin, W. (2020). Youth media consumption and privacy risks in the digital era . In M. Filimowicz & V. Tzankova (Eds.), *Reimagining communication: Experience* (Vol 2, Chapter 12, pp. 195-208). Routledge.

Singh, A., & Singh, S. K. (2019). Technology revolution gives cybercrime a boost: Cyber-attacks and cybersecurity. *International Journal of Advance Computational Engineering and Networking (IJACEN), 7*(8), 5-9. https://iraj.in/journal/IJACEN/paper_detail.php?paper_id=15929&name=Technology_Revolution_gives_Cybercrime_a_Boost:_Cyber-Attacks_and_Cyber_Security

Tabachnick, B. G., & Fidell, L. S. (2013). *Using multivariate statistics* (6th ed.). Pearson.

Tang, Z., Miller, A. S., Zhaou, Z., & Warkentin, M. (2021). Does government social media promote users information security behavior towards COVID-19 scams? Cultivation effects and protective motivations. *Government Information Quarterly*, *38*(2), 101572.

Tsang, M. M., Ho, S. C., & Liang, T. P. (2004). Consumer attitudes toward mobile advertising. *International Journal of Electronic Commerce, 83*(3), 65-78.

Vance, A., Siponen, M., & Pahnila, 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

Vasenska, I., Dimitrov, P., Davidkova, B. K., Krastev, V., Durana, P., & Paulaki, I. (2021). Financial transitions using FINTECH during the COVID-19 crisis in Bulgaria. *Risks*, *9*(3), 48. https://doi.org/10.3390/risks9030048

Wagen, W. V. D., & Pieters, W. (2020). The hybrid victim: Reconceptualizing high-tech cyber victimization through actor-network theory. *European Journal of Criminology, 17*(4), 480-497.

*World Health Organisation* (WHO). (2020, March 11). WHO Director-General's opening remarks at the media briefing on COVID-19 - 11 March 2020. https://www.who.int/director-general/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---11-march-2020

Zarouali, B., Poels, K., Ponnet, K. & Walrare, M. (2018). Everything under control? Privacy control salience influences both critical processing and perceived persuasiveness of targeted advertising among adolescents. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 12*(1). https://doi.org/10.5817/CP2018-1-5