JURNAL PENGGUNA MALAYSIA
MALAYSIAN JOURNAL OF CONSUMER

MACFEA
PERSATUAN EKONOMI PENGGUNA DAN KELUARGA MALAYSIA

JILID 1, VOL 41 **DIS 2025** **eISSN 3030 - 5799**

Tingkah Laku Pembelian Mahasiswa Institusi Pengajian Tinggi dalam Jualan Secara Langsung di Aplikasi Tiktok
Ezni Nazzira Azhar, Nur Ajera Najiha Rosli, Normarshitah Norshahidy dan Siti Yuliandi Ahmad

Emotional Eating, Emotional Food Choice and Its Associated Factors among Public University Students in Malaysia
Nur Shafiqah Azlan, Asma' Ali, Noor Salihah Zakaria, Wan Hafiz Wan Zainal Sukri, Mohamad Rahijan Abdul Wahab and Lee Yi Chen

Intertwined Vulnerabilities: A Conceptual Framework of Food Insecurity, Diet Quality, and Mental Distress among Socioeconomically Disadvantaged University Students in Malaysia
Dhia Widyan Baharuddin, Lee Yi Chen, Abdul Mutalib Embong, Wan Zulkifli Wan Kassim Muhammad Zuhaili Suhaimi, Mohd Radhi Abu Shahim, Shamsul Azahari Zainal Badari, and Muhamad Khairul Zakaria

Factors Influencing Purchase Intention Towards Natural Cosmetics among Students in Universiti Putra Malaysia
Goh Dah Hong and Syuhaily Osman

A Study on Consumers' Cybersecurity Awareness, Threat Perception and Cybersecurity Behaviour in Klang Valley, Malaysia
Ngo Zhen Hong, Syuhaily Osman, Elistina Abu Bakar and Nur Izura Udzir

Linking Knowledge, Awareness and Shopping Habits: A Pathway to Reducing Household Food Waste
Ismawati Sharkawi and Nurul Aiman Idrus

Consumer Demand for Sugar-Sweetened Beverages in Malaysia: Evidence from Brand and Lifestyle Factors
Nor Asmat Ismail and Raihani Nabila Jumadi

The Development of the Prepared Dishes Industry during the Covid-19 Pandemic in China
Zhang Ran and Doris Padmini Selvaratnam

JURNAL PENGGUNA MALAYSIA
(Malaysian Consumer and Family Economics Association)

EDITORIAL BOARD

JURNAL PENGGUNA MALAYSIA adalah keluaran Persatuan Ekonomi Pengguna dan Keluarga Malaysia. Ia bertujuan untuk menyebar, menambah dan berkongsi maklumat berkaitan hal ehwal, undang-undang, penyelidikan dan isu semasa pengguna. Jurnal ini juga menggalakkan penulisan dan perkongsian idea tentang masalah dan keperluan pengguna dalam bentuk rencana, ulasan dan penyelidikan. Sila rujuk panduan kepada penulis untuk penghantaran bahan artikel

Ketua Editor,
Jurnal Pengguna Malaysia
d/a Jabatan Pengurusan Sumber dan Pengajian Pengguna
Fakulti Ekologi Manusia, Universiti Putra Malaysia
43400 UPM Serdang, Selangor
Emel: macfea.upm@gmail.com

JURNAL PENGGUNA MALAYSIA

MACFEA
PERSATUAN EKONOMI PENGGUNA DAN KELUARGA MALAYSIA

JILID 1, VOL 41 | DIS 2025 | eISSN 3030 - 5799 | Halaman

Tingkah Laku Pembelian Mahasiswa Institusi Pengajian Tinggi dalam Jualan Secara Langsung di Aplikasi Tiktok 1
Ezni Nazzira Azhar, Nur Ajera Najiha Rosli, Normarshitah Norshahidy dan Siti Yuliandi Ahmad

Emotional Eating, Emotional Food Choice and Its Associated Factors among Public University Students in Malaysia 22
Nur Shafiqah Azlan, Asma' Ali, Noor Salihah Zakaria, Wan Hafiz Wan Zainal Sukri, Mohamad Rahijan Abdul Wahab and Lee Yi Chen

Intertwined Vulnerabilities: A Conceptual Framework of Food Insecurity, Diet Quality, and Mental Distress among Socioeconomically Disadvantaged University Students in Malaysia 41
Dhia Widyan Baharuddin, Lee Yi Chen, Abdul Mutalib Embong, Wan Zulkifli Wan Kassim, Muhammad Zuhaili Suhaimi, Mohd Radhi Abu Shahim, Shamsul Azahari Zainal Badari and Muhamad Khairul Zakaria

Factors Influencing Purchase Intention towards Natural Cosmetics among Students in Universiti Putra Malaysia 59
Goh Dah Hong and Syuhaily Osman

A Study on Consumers' Cybersecurity Awareness, Threat Perception and Cybersecurity Behaviour in Klang Valley, Malaysia 79
Ngo Zhen Hong, Syuhaily Osman, Elistina Abu Bakar and Nur Izura Udzir

Linking Knowledge, Awareness and Shopping Habits: A Pathway to Reducing Household Food Waste 104
Ismawati Sharkawi and Nurul Aiman Idrus

Consumer Demand for Sugar-Sweetened Beverages in Malaysia: Evidence from Brand and Lifestyle Factors 120
Nor Asmat Ismail and Raihani Nabila Jumadi

The Development of the Prepared Dishes Industry during the Covid-19 Pandemic in China 142
Zhang Ran and Doris Padmini Selvaratnam

PENYUMBANG ARTIKEL

Asma' Ali	Faculty of Fisheries and Food Science, Universiti Malaysia Terengganu
Dhia Widyan Baharuddin	Faculty of Fisheries and Food Science, Universiti Malaysia Terengganu
Doris Padmini Selvaratnam	Faculty of Economics and Management, Universiti Kebangsaan Malaysia
Elistina Abu Bakar	Faculty of Human Ecology, Universiti Putra Malaysia
Ezni Nazzira Azhar	Kulliyyah Pelancongan Mampan dan Bahasa Kontemporari, Universiti Islam Antarabangsa Malaysia
Goh Dah Hong	Faculty of Human Ecology, Universiti Putra Malaysia
Ismawati Sharkawi	Faculty of Humanities, Management and Sciences, Universiti Putra Malaysia, Sarawak
Lee Yi Chen	Faculty of Fisheries and Food Science, Universiti Malaysia Terengganu
Mohamad Rahijan Abdul Wahab	Faculty of Fisheries and Food Science, Universiti Malaysia Terengganu
Mohd Radhi Abu Shahim	Faculty of Business, Economics and Social Development, Universiti Malaysia Terengganu
Muhamad Khairul Zakaria	Centre for Fundamental and Continuing Education, Universiti Malaysia Terengganu
Ngo Zhen Hong	Faculty of Human Ecology, Universiti Putra Malaysia
Noor Salihah Zakaria	Faculty of Fisheries and Food Science, Universiti Malaysia Terengganu
Nor Asmat Ismail	School of Social Sciences, Universiti Sains Malaysia
Normarshitah Norshahidy	Kulliyyah Pelancongan Mampan dan Bahasa Kontemporari, Universiti Islam Antarabangsa Malaysia
Nur Ajera Najiha Rosli	Kulliyyah Pelancongan Mampan dan Bahasa Kontemporari, Universiti Islam Antarabangsa Malaysia
Nur Izura Udzir	Faculty of Computer Science and Information Technology, Universiti Putra Malaysia
Nur Shafiqah Azlan	Faculty of Fisheries and Food Science, Universiti Malaysia Terengganu
Nurul Aiman Idrus	Faculty of Humanities, Management and Sciences, Universiti Putra Malaysia, Sarawak
Raihani Nabila Jumadi	School of Social Sciences, Universiti Sains Malaysia
Shamsul Azahari Zainal Badari	Fakulti Ekologi Manusia, Universiti Putra Malaysia
Siti Yuliandi Ahmad	Kulliyyah Pelancongan Mampan dan Bahasa Kontemporari, Universiti Islam Antarabangsa Malaysia Faculty of Human Ecology, Universiti Putra Malaysia
Syuhaily Osman	Sustainable Consumption Research Group, Faculty of Human Ecology, Universiti Putra Malaysia
Wan Hafiz Wan Zainal Sukri	Faculty of Fisheries and Food Science, Universiti Malaysia Terengganu
Wan Zulkifli Wan Kassim	Centre for Fundamental and Continuing Education, Universiti Malaysia Terengganu
Zhang Ran	Faculty of Economics and Management, Universiti Kebangsaan Malaysia

A STUDY ON CONSUMERS' CYBERSECURITY AWARENESS, THREAT PERCEPTION AND CYBERSECURITY BEHAVIOUR IN KLANG VALLEY, MALAYSIA

Ngo Zhen Hong[1]
Syuhaily Osman*[1]
Elistina Abu Bakar[1]
Nur Izura Udzir[2]

*Corresponding author: (email: syuly@upm.edu.my)

Abstract

Malaysia's cybersecurity incidents are a persistent issue, and human error remains a major contributing factor. This signifies the necessity of understanding an individual's cybersecurity behaviour to avoid negative consequences resulting from cyber threats. However, existing literature on cybersecurity behaviour predominantly focused on organisational settings. Studies addressing cybersecurity behaviour among Malaysian consumers in a non-organisational context remain scarce. Hence, this study aims to explore the current cybersecurity awareness, threat perception and cybersecurity behaviour of consumers in Klang Valley. This study implemented a quantitative approach via cross-sectional study by collecting data through questionnaire distribution. This research obtained 408 valid samples. The findings revealed that consumers in Klang Valley generally share the same consensus regarding privacy concerns and exhibited an overall moderately high level of cybersecurity behaviour. The majority of respondents have a basic understanding of cybersecurity and are moderately interested in attending cybersecurity advocacy programs. Internet sources were acknowledged as the main source of acquiring cybersecurity knowledge. The research seeks to contribute by providing empirical evidence on consumers' cybersecurity behaviour in Klang Valley. These findings are expected to provide additional insights for formulating relevant strategies and policies to mitigate cyber threats.

Keywords: Cybersecurity behaviour; Cyber threats; Consumers; Klang Valley

Abstrak

Kejadian keselamatan siber Malaysia merupakan isu yang berterusan dan kesilapan manusia kekal sebagai faktor penyumbang utama. Ini menandakan keperluan untuk

[1]Department of Resource Management and Consumer Studies, Faculty of Human Ecology, Universiti Putra Malaysia
[2]Department of Computer Science, Faculty of Computer Science and Information Technology, Universiti Putra Malaysia

memahami tingkah laku keselamatan siber individu demi mengelakkan kesan negatif akibat ancaman siber. Namun, literatur semasa berkenaan tingkah laku siber kebanyakkannya tertumpu pada tetapan organisasi. Kajian mengenai tingkah laku keselamatan siber dalam kalangan pengguna Malaysia dalam konteks bukan organisasi masih terhad. Oleh itu, kajian ini bertujuan untuk meneroka keadaan semasa tentang kesedaran keselamatan siber, persepsi ancaman dan tingkah laku keselamatan siber dalam kalangan pengguna di Lembah Klang. Kajian ini telah dilaksanakan dengan pendekatan kuantitatif melalui kajian keratan rentas serta mengumpul data melalui pengedaran soal selidik. Kajian ini telah memperolehi 408 sampel yang sah. Penemuan kajian ini mendedahkan bahawa pengguna di Lembah Klang secara umumnya mempunyai konsensus yang sama terhadap kebimbangan privasi dan telah mempamerkan tahap sederhana tinggi bagi tingkah laku keselamatan siber. Majoriti responden mempunyai sekurang-kurangnya pemahaman minimum tentang keselamatan siber dan minat yang sederhana untuk menghadiri program advokasi keselamatan siber. Sumber Internet telah diakui sebagai sumber utama untuk memperoleh pengetahuan keselamatan siber. Kajian ini bertujuan untuk menyumbang dengan menyediakan bukti empirikal mengenai tingkah laku keselamatan siber pengguna di Lembah Klang. Penemuan ini dijangka memberikan pandangan tambahan dalam perangkaan strategi dan dasar yang berkaitan demi mengurangkan ancaman siber.

***Kata kunci**: Tingkah laku keselamatan siber; Ancaman siber; Pengguna; Lembah Klang*

Introduction

Malaysia is a successful developing country with the adoption of the Internet. People are using it to carry out daily activities, including working, gathering information, shopping, socialising and entertaining themselves. Consumers are also relying on the internet to fulfil daily tasks (Muniandy et al., 2017; Zwilling et al., 2022). As Malaysia advances by adopting technologies and normalising digital services into daily lives, consumers are exposed to the digital world. This opens an opportunity for cyber criminals to perform crime (Muniandy et al., 2017). Based on the statistics from the Malaysia Computer Emergency Response Team (MyCERT) website, there are a total of 7,292 reported incidents related to cybersecurity, such as fraud, spam, intrusion attempts, etc. This caused nearly RM600 millions of losses in the year of 2022. Ministry of Domestic Trade and Consumer Affairs (KPDNHEP) also reported losses amounting to RM21.7 million regarding online fraud. In the years of COVID-19, consumers relied on the Internet most of the time due to restrictions on movement. Concurrently, the cybersecurity incidents escalated to 10,790 cases in 2020 and 10,016 cases in 2021. Among all the different types of cybersecurity incidents, cases related to fraud remained the highest number over the years.

Several studies pointed out that the human error factor is the weakest point in cybersecurity (Alavi et al., 2016; Alsharida et al., 2023; Ariffin et al., 2022). Human mistakes in cyber decision-making can cause cybersecurity problems. Supayah & Ibrahim (2016) also concluded that human error is a major contributing factor to cybersecurity in Malaysia. Therefore, there are many indications that signify the necessity of understanding an individual's cybersecurity behaviour to avoid negative consequences of cyber threats (Alshamrani et al., 2019; Shappie et al., 2020; Thompson et al., 2017; Tsai et al., 2016; Zwilling et al., 2022). Nevertheless, a broader understanding of consumers' cybersecurity behaviour is crucial to assist in diminishing the effect of cyber threats (Butavicius et al., 2020; Shappie et al., 2020; Zwilling et al., 2022). Accordingly, this study endeavoured to explore the current cybersecurity awareness, threat perception and cybersecurity behaviour among consumers in Klang Valley to develop a fundamental understanding regarding consumers' cybersecurity.

Literature Review

Among the Risk and Five Hard Problems of Cybersecurity proposed by Scala et al. (2019), the statement of "understanding and accounting for human behaviour" indicates the importance of the human being's role in understanding cybersecurity behaviour. Plentiful research also evidenced that the human error factor is the weakest point in cybersecurity (Alavi et al., 2016; Ariffin et al., 2022). This is due to the human error factor leads to cybersecurity problems. Therefore, it is crucial to understand an individual's cybersecurity behaviour to mitigate the consequences of cyber threats (Alshamrani et al., 2019; Shappie et al., 2020; Thompson et al., 2017; Tsai et al., 2016; Zwilling et al., 2022).

There is a distinction between traditional cybersecurity and the study of cybersecurity behaviour. Traditional cybersecurity studies emphasise technical aspects such as software intrusion, anti-virus and firewalls (Barletta et al., 2024). On the other hand, cybersecurity behavioural studies focus on a human-centred approach and involve investigation into the invasion mechanism related to human behaviour (Baltuttis et al., 2024; Chowdhury et al., 2020; Dalal et al., 2022; Pollini et al., 2022). Cybersecurity behaviour refers to an individual's action to actively avoid cyber threats by performing cybersecurity practices (Alanazi et al., 2022; Hong & Furnell, 2021). Due to the acknowledgements of human factor as an issue in cybersecurity, cybersecurity behavioural studies are emerging in different contexts and perspectives (Baltuttis et al., 2024).

Studies regarding the cybersecurity behaviour of organisational workers have received considerable attention. For instance, several studies examined potential underlying psychological processes influencing employees' cybersecurity behaviour, such as work overload (Kim & Kim, 2024) and time pressure (Chowdhury et al., 2020).

Another study has explored the dimensions of cybersecurity behaviour, identified cybersecurity user types in the workplace and developed measurement instruments specifically to understand employees' cybersecurity behaviour (Baltuttis et al., 2024). Previous studies have also explored the factors that contribute to risky behaviour in the workplace (Anwar et al., 2017; Gillam & Foster, 2020; Hadlington, 2017). Furthermore, individual differences such as gender have also been considered, which are associated with cybersecurity behaviour in organisations (Anwar et al., 2017; Beu et al., 2023).

Research on consumer-level cybersecurity behaviour is emphasised primarily in the education sector (Alsharida et al., 2023). For instance, several cybersecurity behaviour studies of academic staff are found to be influenced by knowledge, attitude, awareness and institutional culture (Badreddine et al., 2025; Gushelmi et al., 2024; Mamade & Dabala, 2021). Besides that, several studies have also inculcated students' involvement in cybersecurity behaviour-based studies (Alanazi et al., 2022; Khan et al., 2022; Matyokurehwa et al., 2021). Furthermore, recent studies regarding cybersecurity behavioural aspects among Metaverse users have also attracted scholars' interest (Al-Emran et al., 2024; Alsharida et al., 2025). This is due to the emerging technology advancement of Metaverse products such as augmented reality (AR), virtual reality (VR) and advanced web platform (Dwivedi et al., 2022), which give rise to privacy concerns (Koohang et al., 2023).

However, research on cybersecurity behaviour has been more rigorous and productive in organisational settings. This is due to the higher vulnerability of organisations to cyber threats, which requires greater investment in prevention measures (Alsharida et al., 2023). In contrast, studies at the consumer level remain relatively scarce and scattered in existing literature. Despite the attention given to cybersecurity behaviour in organisational settings, the countermeasures provided, such as campaigns, training and stimulated events, are proven to be ineffective as referred from the rising incident statistics (Baltuttis et al., 2024; Dalal et al., 2022). A recent meta-analysis concludes the inability of current cybersecurity training approaches to influence individuals' behaviour (Prümmer et al., 2025). Besides that, cyber-attacks between organisational settings and non-organisational settings are different. Consumers in a non-organisational environment who possess lower adoption of protection measures and experiences are more likely to be vulnerable when encountering cyber threats (Hong & Furnell, 2021).

Furthermore, to the best of our knowledge, research regarding cybersecurity behaviour in Malaysia is limited. A study on government servants and online banking users in Malaysia who practice cybersecurity possesses high severity, vulnerability, response efficacy and self-efficacy level (Sulaiman et al., 2022; Vafaei-Zadeh et al., 2025). Moreover, a study on 340 tertiary students suggested demographic characteristics – age, gender and education level are significant mediators of

cybersecurity behaviour (Fatokun et al., 2019). Another study involving 450 tertiary students in Klang Valley established associations between cybersecurity behaviour and several validated cybersecurity factors (Fatokun Faith et al., 2020). To date, there are no studies that systematically examine cybersecurity awareness, threat perception and cybersecurity behaviour in the general consumer context in Malaysia.

As cyber incident statistics in Malaysia remained at a significant amount, the necessity to understand cybersecurity behaviour among consumers is imperative. This is because a deficiency in possessing relevant cybersecurity behaviour leads to falling victim to cyber threats (Mohammad et al., 2022). Moreover, most studies have focused on organisational cybersecurity, and little is known about consumer-level cybersecurity behaviours in Malaysia. Therefore, the study aims to explore current cybersecurity awareness, threat perception and cybersecurity behaviour among consumers in Klang Valley. The current topic warrants an investigation to provide a general insight into the existing situation pertinent to cybersecurity in Malaysia's consumer context.

Methodology

The study implemented a cross-sectional study by collecting data through questionnaire distribution. As literature regarding consumers' cybersecurity in Malaysia is scarce, a cross-sectional study is conducted. This is an effective method to quickly gather data in a single period of time (Wang & Cheng, 2020). A cross-sectional study is suitable for the current study as it provides a wide coverage in numerous areas in human behaviour, conditional and population studies (Connelly, 2016).

In general, a total of 424 respondents were selected to complete a set of self-administered questionnaires. This particular number of samples is acquired based on a comparison of several sample size determination methods to ensure adequate sample size. This study utilised Krejcie and Morgan's table (Krejcie, R. J. & Morgan, D. W., 1970), Raosoft sample size calculator (Raosoft, Inc., 2004), Sample-to-variable ratio (Hair Jr. et al., 2019) and power analysis with G*Power software (Erdfelder et al., 2009; Faul et al., 2007, 2009). Lastly, an inclusion of 10% additional samples upon consideration of possible withdrawals, missing data and follow-up failures in data collection. The determination method of 424 samples based on the respective sample size determination methods is summarised in Table 1.

Table 1: Sample Size Determination Methods

Sample Size Determination Method	Suggested Sample Size	Implemented Sample Size
Krejcie and Morgan's Table	384	385
Raosoft (95% confidence interval)	385	
Sample-to-variable Ratio	160	
G*Power (effect size = 0.15, α = 0.05 and power = 0.80)	114	
Add: 10% additional samples		385 x 10% = 38.5 (39)
Total		**424**

The sampling technique implemented in this research is multistage sampling. During the first stage, Klang Valley is selected through purposive sampling due to its suitability for the current study objectives (discussed in the next paragraph). Subsequently, 4 districts of Klang Valley – Petaling, Klang, Ulu Langat and Putrajaya were selected through simple random sampling. Followingly, proportionate stratified random sampling is implemented, and 106 were targeted to be collected for each respective district. Next, simple random sampling is applied to select one mall in each chosen district, which will serve as the starting point for data collection. Lastly, a systematic sampling method is implemented by selecting each 5th sampling unit consecutively to inquire their willingness to participate in the study. In simpler terms, every 5th person who enters or exits the mall entrance is chosen to ask for their interest to complete the questionnaire.

Klang Valley is chosen as the study location for this study due to its categorisation as one of the metropolitan areas in Malaysia. Moreover, it encompasses highest Internet adoption rate among consumers (Department of Statistics Malaysia (Department of Statistics Malaysia, 2023). As the current study focuses on the cybersecurity context, the researcher acknowledged that the research location should focus on areas with the highest cybercrime rate. However, after extensive data acquisition, there are no exact statistics of cybercrime and fraud according to the states at the moment. Hence, this current research takes into account areas with the highest Internet adoption rate. This is because a higher Internet adoption rate with longer usage hours posits a higher probability of confronting threats (Tuptuk & Hailes, 2018).

Research Instrumentation

The questionnaire consists of three sections, and the measurement items were adopted and adapted from governmental surveys as well as previous studies. The constructed measurement items are validated by several experts in the field of behavioural, humanities and cybersecurity studies. Section A encompasses respondents' socio-demographic characteristics, including gender, age, ethnicity, marital status, education level, employment status and household monthly income

category. This section consists of five closed-ended questions and one open-ended question. Closed-end questions allow respondents to answer by selecting the preferred choice of selection, such as a multiple-choice question, whereas open-ended questions allow respondents to give short answers or an essay to best describe themselves (Hyman, M. R., & Sierra, 2016). In this case, the five closed-ended questions are ethnicity, gender, highest level of education, employment status and household monthly income category, whereas age is the only open-ended question in this section.

Section B consisted of general questions on cybersecurity and respondents' familiarity with cyber threats. The questions in this section included familiarity with the "cybersecurity" term, interest in attending a cybersecurity advocacy program/training, sources of obtaining cybersecurity knowledge, cyber threats, previous experience in encountering situations where cyber threats may potentially occur, as well as the frequency of encountering them. These questions were adapted and modified from the Malaysian government survey – ICT Use and Access by Individuals and Household Survey Report 2022. The questions adopted a nominal scale, an ordinal scale and multiple answer options. Respondents were asked to select the answers that best relate to them based on their perception and experiences.

Lastly, Section C consisted of 17 measurement items to assess an individual's cybersecurity behaviour. Current section encompasses numerous different constructs - password management, email usage, internet usage, social media usage, mobile devices, information handling, incident reporting, software updating and network management. The measurement scale for the current study is adapted from Baltuttis et al. (2024), with a pilot-tested Cronbach Alpha value of 0.891. The current section employed a 7-point Likert scale ranging from 1 (Strongly Disagree) to 7 (Strongly Agree). The negative statements in this section were noted and reverse-coded before commencing data analysis. A higher score acquisition indicates a higher engagement in cybersecurity activities. The classification of the cybersecurity behavioural scale and engagement level is presented in Table 2.

Table 2: Classification of Cybersecurity Behaviour Scale and Engagement Level

Score	7-point Likert scale	Engagement Level
1	Strongly Disagree	Extremely Low
2	Disagree	Low
3	Somewhat Disagree	Moderately Low
4	Neutral	Moderate
5	Somewhat Agree	Moderately High
6	Agree	High
7	Strongly Agree	Extremely High

Ethical Statements

This study received approval from the university's board of ethics reviewer on 18 December 2024 (Reference No.: JKEUPM-2024-892). This study confirms that the research procedure was performed in alignment with principles expressed in the Declaration of Helsinki (2008). Informed consent was given to all participants upon agreeing to participate in this study. An informed consent form is first presented to the respondents before the actual survey begins. The informed consent form includes details such as a brief introduction of the study, exclusion criteria, benefits for subjects, and the investigators' as well as researchers' contact information. Respondents are also informed of the anonymity, voluntary participation and freedom to withdraw at any point in time. Furthermore, there are no foreseeable risks associated with this study. Upon agreeing to participate and acknowledging data usage for publication, the consent form was signed by the respondents through pen hand paper.

Results and Discussion

Respondent's Demographic Characteristics

The study received a valid sample return rate of 96.23%, with 408 complete responses out of 424 collected samples. The demographic characteristics of respondents with valid responses are presented in Table 3, which encompasses gender, age, ethnicity, education level, employment status and household income categories.

Table 3: Respondents' Demographics Characteristics, N = 408

Characteristics	Frequency (n)	Percentage (%)
Gender		
Male	183	44.9
Female	225	55.1
Age		
18 – 30 years old	255	62.5
31 – 40 years old	66	16.2
41 – 50 years old	48	11.8
51 – 60 years old	29	7.1
Above 60 years old	10	2.5

Table 3 (continued)

Characteristics	Frequency (n)	Percentage (%)
Ethnicity		
Malay	210	51.5
Chinese	118	28.9
Indian	53	13.0
Bumiputera Sabah/Sarawak	20	4.9
Others	7	1.7
Marital status		
Single	259	63.5
Married	132	32.4
Widowed	9	2.2
Divorced	8	2.0
Education level		
Primary school	9	2.2
LCE/SRP/PMR/PT3	21	5.1
SPM/MCE	86	21.1
STPM/HSC	16	3.9
Skills Certificate (SKM)	11	2.7
Diploma	36	8.8
Bachelor's Degree	213	52.2
Master or Ph.D.	16	3.9
Employment status		
Government employee	40	9.8
Private employee	220	53.9
Self employed	22	5.4
Unemployed	24	5.9
Student	98	24.0
Retired	4	1.0
Household income category		
Less than RM3,440	177	43.4
RM3,440 – RM5,249	116	28.4
RM5,250 – RM7,689	57	14.0
RM7,690 – RM11,819	36	8.8
RM11,820 and above	22	5.4

As reported in Table 3, there were 44.9 percent males and 55.1 percent females. The majority were aged between 18 – 30 years old (62.5%), with great participation support from Malays (51.5%), followed by Chinese (28.9%) and Indians (13.0%). Most respondents were single (63.5%), and half of the respondents had attained at least a bachelor's degree (52.2%). For employment status, the majority of the respondents were employed in the private sector (53.9%). Lastly, 43.4 percent of respondents reported household income less than RM3,440, followed by 28.4 percent of respondents who reported household income ranging between RM3,440 and

RM5,249. This indicates that the majority of the respondents who participated in the study fall under the low-income household group - B40 (Department of Statistics Malaysia, 2022).

General Insights of Cybersecurity Awareness, Threat Perception and Cybersecurity Behaviour Among Consumers in Klang Valley

A descriptive analysis of general insights of respondents' cybersecurity awareness, threat perception and experiences is presented in Table 4 – 6. Table 4 reflected respondents' term familiarity with "cybersecurity" and interest in attending cybersecurity-related programs by adopting a 5-point ordinal scale. Table 5 presents respondents' sources of cybersecurity knowledge, cyber threat perception and situations encountered where the occurrence of cyber threats may arise. The questions were treated as a multiple-response item, allowing respondents to select the best, indicating their view of thoughts. Lastly, Table 6 assessed respondents' frequency of risk situations in encountering cyber threats by adopting a 4-point ordinal scale.

Table 4: Respondents' Cybersecurity Awareness: Familiarity with Terms and Advocacy Interest, N = 408

Item	Number of Respondent (n)	Percentage (%)
(1) Are you familiar with the term "cybersecurity" before filling this survey?		
Not at all	31	7.6
Slightly	97	23.8
Moderately	166	40.7
Very	84	20.6
Extremely	30	7.4
(2) Are you interested in attending cybersecurity advocacy program/training if there is any?		
Not at all	54	13.2
Slightly	66	16.2
Moderately	149	36.5
Very	98	24.0
Extremely	41	10.0

Based on Table 4, the majority of the respondents reported a moderate level of familiarity with the term (40.7%). Similarly, the majority of respondents are moderately interested in engaging in cybersecurity advocacy programs (36.5%). For familiarity with the "cybersecurity" term, there are only 7.6 percent who have no familiarity with the term. This indicates that most of the respondents have at least a minimum level of

understanding towards cybersecurity (92.4%). On the other hand, the findings also revealed that only a small proportion of respondents reported having no interest in attending a cybersecurity advocacy program (13.2%). Meanwhile, a slightly higher proportion of 16.2 percent of respondents reported having a slight interest. This suggests that the majority of respondents have having moderate or higher interest in attending cybersecurity-related advocacy programs (70.5%). Hence, this reflects a generally positive baseline of cybersecurity awareness, which can be leveraged for future consumer-targeted advocacy programs. Policymakers and consumer associations may focus on strengthening advocacy strategies in raising cybersecurity awareness. Concurrently, future program design can also be considered to foster more consumer involvement in cybersecurity practices.

Table 5: Respondents' Sources of Cybersecurity Knowledge, Cyber Threat Perception and Encounters (Multiple Choice Responses), N = 408

Items	Frequency (n)	Percentage of Respondents (%)
(3) Where do you obtain knowledge on cybersecurity?		
Internet sources	335	82.1
School classes	127	31.1
Conferences/Seminars/Workshops/Advocacy program/Forum	124	30.4
Conventional media (newspaper, magazines, TV, radio etc.)	212	52.0
Journal articles	72	17.6
Industry reports	66	16.2
Talking with family/friends	240	58.8
Victim of cyber attack	45	11.0
None	17	4.2
(4) In your opinion, which of the following is/are considered cybersecurity threats to you?		
Blocking access to information	201	49.3
Violation of your privacy	361	88.5
Loss of data (personal, work etc.)	334	81.9
Loss of money	355	87.0
Device damage	169	41.4
Spying on you	300	73.5
Spying on your organization	152	37.3
Takeover of your device control	217	53.2
Blocking your business process	120	29.4
Misuse of your personal information	301	73.8

Table 5 (continued)

Items	Frequency (n)	Percentage of Respondents (%)
(5) Which of the following situation(s) have you encountered?		
Received email from unknown senders	188	46.1
Received "new" friend request(s) from unknown people in social media (without any mutual friends/followers)	336	82.4
Received messages with URL links from unknown people	208	51.0
Received request to download files / apps	148	36.3
Received requests for banking account / password / TAC code	95	23.3
Received requests to pay on non-banking apps	82	20.1
Being cyber blackmailed	63	15.4
Being forcefully downloaded unknown files/apps	128	31.4
Being forcefully directed to unknown websites/pop-ups	218	53.4
Being forcefully added into unknown groups in social apps (WhatsApp, Facebook Messenger, Instagram chats etc.)	347	85.0
Being locked out from computer system and forced to pay	31	7.6
Being impersonate by other people	92	22.5
Have not encountered any	10	2.5

Note: Participants could select more than one option. Percentages are calculated based on the total number of respondents (n=408) for each option given.

Cybersecurity Knowledge

Table 5 portrays multiple-choice items to assess respondents' sources of cybersecurity knowledge, cyber threat recognition and situations encountered. For sources of acquiring cybersecurity knowledge, most of the respondents reported internet sources (82.1%) as their medium of understanding cybersecurity. Subsequently, the findings also revealed that approximately half of the respondents understand cybersecurity by talking with family or friends (58.8%) and also through conventional media (52.0%). These findings suggested the significant role of media and social circles in effectively promoting cybersecurity awareness and obtaining information.

Social media are significant sources of information as people explore and share cybersecurity knowledge (Patnayakuni et al., 2018). Additionally, it also serves as an electronic word of mouth, potentially reaching to wide audience over time (Vanderkooi et al., 2023). Hence, it is also likely that Malaysian consumers utilised social media to share or receive information from family members and friends (Ishak et al., 2020; Kuok Tiung et al., 2016), including cybersecurity knowledge. Moreover, the

dissemination of cybercrime issues through conventional media has also contributed partially to raising awareness. This is because these media rely heavily on government sources for cybersecurity information, thus fostering prevention and intervention measures (Wen et al., 2025).

Threat Perception

The majority of the respondents recognise violation of privacy (88.5%), loss of money (87.0%) and loss of personal or work data (81.9%) as cyber threats. Furthermore, there are also a significant number of respondents who considered misuse of their personal information (73.8%) and spying on them (73.5%) as cyber threats. This indicates that consumers in Klang Valley mostly give serious consideration to their personal privacy and financial assets. Meanwhile, there is a low attention given to business and organisation-related cyber threats. Only 37.3 percent of respondents marked cyber threats for spying on their organisation, and 29.4 percent of them marked blocking business processes. However, it is important to note that low recognition of business-related threats may be attributable to different characteristics of the sampled population. The respondents in this study represent consumers rather than business owners. This interpretation could be evidenced by the employment in Table 2, which indicates that the majority of the respondents are currently employed in the private sector. Exposure to business processes may be limited among the current samples.

Cyber Threat Situation Encounters

In regard to the situations encountered where the occurrence of cyber threats may arise, the majority of respondents (85.5%) encountered being forcefully added into unknown groups in social apps, such as WhatsApp, Facebook Messenger, Instagram chats and others. Similarly, a similar proportion of respondents (82.4%) also received new friend requests from unknown people on social media. This could be attributed to the ignorance of consumers to cybersecurity hazards (Pal et al., 2023). There is also a high possibility that consumers may unintentionally disclose their personal information, which provides criminals the opportunity to stalk or misuse (Choi et al., 2013). As a result, the exploited information is often used by hackers to bypass security mechanisms (Pal et al., 2023). This further leads to forcefully adding users to a group to spread malicious content.

Table 6: Respondents' Frequency of Cyber Threats Risk Encounters, N = 408

Item	Number of Respondent (n)	Percentage (%)
(6) Followed by (5), how often do you encounter those situation(s)?		
Never	11	2.7
Seldom	179	43.9
Sometimes	181	44.4
Often	37	9.1

As presented in Table 6, respondents who marked “seldom” and “sometimes” were nearly equal, reported at 43.9 percent and 44.4 percent, respectively. Subsequently, 9.1 percent of respondents have reported often encountering such situations. This indicates that over 97% of the respondents’ encountered situations where cyber threats may potentially occur. This underscores a huge vulnerability among consumers in Klang Valley. This could be due to the high Internet penetration occurring in the Klang Valley. A longer period of online activities may increase the likelihood of consumers being exposed to cyber threat situations (Tuptuk & Hailes, 2018). Furthermore, the proportion of respondents who reported encountering threats ‘seldom’ (43.9%) is substantially higher than those who reported experiencing them ‘often’ (9.1%). This disparity suggests that while cybersecurity threats may not occur frequently for most consumers, however remain an ongoing risk. The high proportion of occasional encounters also reflects a continuous baseline risk that consumers should not ignore.

Descriptive Analysis of Respondents’ Cybersecurity Behaviour

In this study, the cybersecurity behaviour of respondents in Klang Valley was assessed through 17 items. The measurement scale encompasses different constructs, including password management, email usage, internet usage, social media usage, mobile devices, information handling, incident reporting, software updating and network management. The results for the mean and standard deviation for each item are presented in Table 6 for descriptive analysis.

Table 7: Descriptive Statistics of Respondents’ Cybersecurity Behaviour, N = 408

Items	Mean	Standard Deviation
Password management		
I do not share my passwords with others (e.g., colleagues, friends).	6.55	0.848
I use different passwords for different accounts that I have.	4.78	1.725
When I create a new online account, I try to use a password that goes beyond the website’s minimum requirements.	5.66	1.455

Table 7 (continued)

Items	Mean	Standard Deviation
Email use		
I click on email links/attachments from known sources without checking whether it looks suspicious. **	2.66	1.695
I open email attachments from unknown senders. **	2.72	1.675
Internet use		
I download any files into my devices that will help me get the job done. **	3.70	1.770
I do not access the safety of websites before entering information (e.g., URL, HTTPS, certificates). **	3.60	1.957
Social media use		
I avoid uploading related personal information (e.g., identity card, passport, vehicle registration plates, company data) to social media.	6.46	0.822
I regularly review my social media privacy settings.	4.59	1.710
Mobile devices		
I always connect to free Wi-Fi whenever it is available. **	3.71	1.887
I ensure strangers could not see my device screen if I am working on a sensitive document.	5.88	1.275
I disable wireless technologies when not using it.	4.60	1.716
I lock my device screen when I am not using it.	6.04	1.197
Information handling		
I would not plug a USB stick found in public place into my computer.	5.81	1.329
When sensitive printouts need to be disposed of, I ensure that they are destroyed in browser history.	5.61	1.576
Incident reporting		
I report suspicious emails and make spam reporting.	4.92	1.729
Updating		
I update my software regularly.	5.18	1.564

*Note: ** Reverse code items*

As disclosed in Table 7, the item on not sharing passwords with others (e.g. friends, colleagues) has the highest mean score at 6.55. Similarly, the item of avoiding uploading related personal information (e.g., identity card, passport, vehicle registration plates, company data) to social media consisted of a mean score of 6.46. Additionally, the relatively small number of standard deviations of 0.848 and 0.822 respectively suggested that responses for the respective items are fairly consistent across respondents. Subsequently, respondents also reported a high mean score of 6.04 with a slightly higher standard deviation of 1.197 for the item on locking device screen when not using it. This indicates that consumers in Klang Valley generally have concern regarding personal privacy, which is consistent with the conclusion established in Table 5.

The lowest mean score was reported for the item on clicking email links from known sources without checking (M = 2.66, SD = 1.695). The item on open email attachments from unknown senders have a slightly higher mean score of 2.72 with standard deviation of 1.675. However, it is worth highlighting that the respective items were designed in reverse form. After reverse coded for both aforementioned items, respondents generally have a moderate high mean score for both respective items. This indicates that the respondents were generally having a moderate high level of cautious on checking the sources before accessing suspicious email links or attachments.

There are some noteworthy findings that may serve as a basis for further exploration. Respondents demonstrated a moderate level score of proficiency in handling social media and mobile device settings. Both items "I regularly review my social media privacy settings" and "I disable wireless technologies when not using it" reported a nearly equal mean score of 4.59 and 4.60 respectively. This finding revealed that respondents have distinct perceptions and behaviour with respect to social media and mobile devices settings. This further indicates that a proportion of respondents perceive managing settings as irrelevant, resulting in noncompliance with cybersecurity practices. Poor management of privacy settings possessed potential risk to allow third party to gain access to their social media account, further obtaining personal information and compromising contents (Croom et al., 2016; Luo & Ing, 2022). However, there is a possibility that consumers may not be aware of the significance of privacy settings, which result in non-compliance with relevant behaviour (Al-Shdayfat, 2018; Cecere et al., 2015).

Additionally, as majority of the population samples are young consumers, there are other possible explanations. Previous study shows that young adults often stick to default privacy settings to minimize cognitive effort (Choi et al., 2013). Another study established that young adults assumed that privacy violations are acceptable, given the opaque nature of institutions and the technological affordances of social media (Hargittai & Marwick, 2016). This resulted an assumption of beyond control regarding their privacy settings, which further leads to negligence. There are also recent evidence suggesting that young adults often incorrectly assume a more convenient security option to be safe (Ervits & Maintz, 2025). This facilitates the occurrence of security trade off and causing them to forgo some privacy for the convenience of using social media. Hence future research may consider including habitual conveniences and security trade off, especially in the studies of young consumers in cybersecurity context.

As such, there is also an interesting finding that warrants attention. Based on the findings in Table 7, a noticeable difference in mean score is observed across items related to password management. Precisely, not sharing password appears to be a more convenient protective action compared to using different password and creating

password that exceed standard requirements. Evidently, this finding is consistent with earlier discussion. This indicates that young adults indeed prefer a more convenient option with minimal cognitive effort in cybersecurity (Cho et al., 2019; Ervits & Maintz, 2025). A similar pattern can also be observed in social media use category. Moreover, the optimistic bias of young adults may also be a potential factor in influencing the mean score (Onuma et al., 2013). The perceiving of email vigilance and privacy risks as less harmful and inconvenient resulted in lack of verification of legitimacy (Connaway et al., 2011), thereby leads to vulnerabilities. Hence, these findings indicate that cybersecurity advocacy efforts should prioritize weaker domains such as email vigilance, social media privacy settings and wireless use management, rather than password hygiene where compliance is already strong.

Conclusion, Limitations, Recommendations and Contributions

Among the 408 respondents in this study, there were 44.9 percent male and 55.1 percent female. Most of the respondents are aged in between 18 – 30 years old with higher percentage of Malay participants. The study also concluded that respondents who participate in this study had attained at least a bachelor's degree and are mostly employed in the private sector. Lastly, a large proportion of respondents from the low-income household group (B40) participated in the study, which summed up to 71.8 percent.

The findings revealed that majority of consumers in Klang Valley rely on Internet sources (82.1%) for cybersecurity knowledge, while over one-third (36.5%) show a moderate level of interest in attending advocacy programs. Privacy violations, financial losses, and data breaches are widely recognized as major cyber threats. In terms of cyber threat situation encounters, many consumers reported receiving friend requests from strangers and being added to unknown groups on platforms such as WhatsApp, Facebook Messenger, and Instagram. Notably, nearly half of the respondents encountered these situations with some frequency, indicating that such threats remain persistent in consumers' digital interactions.

Despite the findings, the study has limitation that warrant consideration. This research is specifically focused on exploring and examining the cybersecurity awareness, threat perception and cybersecurity behaviour among consumers in Klang Valley. Accordingly, the samples in this study are restricted only to Klang Valley, Malaysia, which affects generalizability. Hence, it is suggested to expand the study to diverse geographical regions and populations to enhance external validity. Furthermore, reliance on self-reported data may introduce potential biases. Future studies may include both observational and self-reporting assessment to achieve greater objectivity of measurements (Li et al., 2022). Besides that, the study adopted cross-sectional research design, which may potentially limit the affirmance of causal relationships between variables of study. Lastly, the collected samples are skewed

toward B40 household income category, which may affect generalizability across middle-income and high-income groups.

The findings highlighted several practical implications for strengthening consumer cybersecurity behaviour. First, integrating cybersecurity awareness into school curriculums is essential, as classroom-based exposure was found to be relatively low. Second, advocacy programs should incorporate scenario-based simulations that address common risks such as phishing, unsafe use of free Wi-Fi, and inadequate privacy settings. This initiative will enable consumers to translate awareness into practical skills. Finally, collaboration with telecommunications providers and Internet service providers could further enhance consumer protection. Incorporating measures such as SMS alerts and phishing warnings helps to ensure effective intervention against potential cyber threats.

This study also offers several key contributions. In terms of theoretical contribution, this study extends cybersecurity behaviour research beyond organizational settings by examining the consumer context in Klang Valley Malaysia. In terms of practical contribution, this study identifies priority areas for intervention, particularly in phishing, email vigilance, and unsafe Wi-Fi practices. From a policy perspective, the findings provide valuable insights for agencies such as Ministry of Domestic Trade and Consumer Affairs (KPDNHEP) and MyCERT in tailoring awareness campaigns to strengthen consumer protection. A comprehension understanding of current circumstances regarding individual's cybersecurity contributes to identify effective strategies to mitigate cyber threats (Alanazi et al., 2022). Hence, future research could build on these insights to further refine cyber threat mitigation strategies at the household and consumer levels.

Acknowledgements

This research was funded under Geran Inisiatif Putra Siswazah (GP-IPS) with project code: GP-IPS/2024/9804700. This grant is supported by Research Management Centre, Universiti Putra Malaysia.

References

Alanazi, M., Freeman, M., & Tootell, H. (2022). Exploring the factors that influence the cybersecurity behaviors of young adults. *Computers in Human Behavior*, *136,* 107376. https://doi.org/10.1016/j.chb.2022.107376

Alavi, R., Islam, S., & Mouratidis, H. (2016). An information security risk-driven investment model for analysing human factors. *Information and Computer Security*, *24*(2), 205–227. https://doi.org/10.1108/ICS-01-2016-0006

Al-Emran, M., Al-Sharafi, M. A., Foroughi, B., Iranmanesh, M., Alsharida, R. A., Al-Qaysi, N., & Ali, N. (2024). Evaluating the barriers affecting cybersecurity behavior in the Metaverse using PLS-SEM and fuzzy sets (fsQCA). *Computers in Human Behavior*, *159,* 108315. https://doi.org/10.1016/j.chb.2024.108315

Alshamrani, A., Myneni, S., Chowdhary, A., & Huang, D. (2019). A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities. *IEEE Communications Surveys and Tutorials*, *21*(2), 1851–1877. https://doi.org/10.1109/COMST.2019.2891891

Alsharida, R. A., Al-rimy, B. A. S., Al-Emran, M., Al-Sharafi, M. A., & Zainal, A. (2025). Predicting cybersecurity behaviors in the Metaverse through the lenses of TTAT and TPB: a hybrid SEM-ANN approach. *Online Information Review*. Advance online publication. https://doi.org/10.1108/OIR-08-2023-0425

Alsharida, R. A., Al-rimy, B. A. S., Al-Emran, M., & Zainal, A. (2023). A systematic review of multi perspectives on human cybersecurity behavior. *Technology in Society*, *73*, 102258. https://doi.org/10.1016/j.techsoc.2023.102258

Al-Shdayfat, N. M. (2018). Undergraduate student nurses' attitudes towards using social media websites: A study from Jordan. *Nurse Education Today*, *66,* 39–43. https://doi.org/10.1016/j.nedt.2018.03.017

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior*, *69*, 437–443. https://doi.org/10.1016/j.chb.2016.12.040

Ariffin, M. A. M., Darus, M. Y., Haron, H., Kurniawan, A., Muliono, Y., & Pardomuan, C. R. (2022). Deployment of Honeypot and SIEM Tools for Cyber Security Education Model in UITM. *International Journal of Emerging Technologies in Learning*, *17*(20), 4–19. https://doi.org/10.3991/ijet.v17i20.32901

Badreddine, S., Alwada'n, T., Razzaque, M. A., Al Kafri, A., Al Ammari, H., & Hamdan, A. (2025). Culture in higher education: An empirical analysis of employee perceptions and behavioural outcomes in the UAE. *Edelweiss Applied Science and Technology*, *9*(5), 1126–1142. https://doi.org/10.55214/25768484.v9i5.7092

Baltuttis, D., Teubner, T., & Adam, M. T. P. (2024). A typology of cybersecurity behavior among knowledge workers. *Computers and Security*, *140*, 103741. https://doi.org/10.1016/j.cose.2024.103741

Barletta, V. S., Caivano, D., Catalano, C., de Gemmis, M., & Impedovo, D. (2024). Cyber social security education. In *Lecture Notes in Computer Science* (Vol.

15030 LNCS, pp. 240–248). Springer. https://doi.org/10.1007/978-3-031-71713-0_16

Beu, N., Jayatilaka, A., Zahedi, M., Babar, A., Hartley, L., Lewinsmith, W., & Baetu, I. (2023). Falling for phishing attempts: An investigation of individual differences that are associated with behavior in a naturalistic phishing simulation. *Computers & Security*, *131*, 103313. https://doi.org/10.1016/j.cose.2023.103313

Butavicius, M., Parsons, K., Lillie, M., McCormac, A., Pattinson, M., & Calic, D. (2020). When believing in technology leads to poor cyber security: Development of a trust in technical controls scale. *Computers & Security*, *98*, 102020. https://doi.org/10.1016/j.cose.2020.102020

Cecere, G., Le Guel, F., & Soulié, N. (2015). Perceived internet privacy concerns on social networks in Europe. *Technological Forecasting and Social Change*, *96*, 277–287. https://doi.org/10.1016/j.techfore.2015.01.021

Cho, H., Roh, S., & Park, B. (2019). Of promoting networking and protecting privacy: Effects of defaults and regulatory focus on social media users' preference settings. *Computers in Human Behavior*, *101*, 1–13. https://doi.org/10.1016/j.chb.2019.07.001

Choi, D., You, I., & Kim, P. (2013). Syntactic analysis for monitoring personal information leakage on social network services: A case study on Twitter. In *Lecture notes in computer science* (Vol. 7804 LNCS, pp. 302–313). Springer. https://doi.org/10.1007/978-3-642-36818-9_26

Chowdhury, N. H., Adam, M. T. P., & Teubner, T. (2020). Time pressure in human cybersecurity behavior: Theoretical framework and countermeasures. *Computers & Security*, *97,* 101931. https://doi.org/10.1016/j.cose.2020.101931

Connaway, L. S., Dickey, T. J., & Radford, M. L. (2011). "If it is too inconvenient, I'm not going after it:" Convenience as a critical factor in information-seeking behaviors. *Library & Information Science Research*, *33*(3), 179–190. https://doi.org/10.1016/j.lisr.2010.12.002

Connelly, L. M. (2016). Cross-sectional survey research. *MEDSURG Nursing*, *25(5), 369–370.*

Croom, C., Gross, B., Rosen, L. D., & Rosen, B. (2016). What's Her Face(book)? How many of their Facebook "friends" can college students actually identify? *Computers in Human Behavior*, *56*, 188–193. https://doi.org/10.1016/j.chb.2015.11.015

Dalal, R. S., Howard, D. J., Bennett, R. J., Posey, C., Zaccaro, S. J., & Brummel, B. J. (2022). Organizational science and cybersecurity: Abundant opportunities for research at the interface. *Journal of Business and Psychology*, *37*(1), 7–26. https://doi.org/10.1007/s10869-021-09732-9

Department of Statistics Malaysia. (2022). *Household income survey report, Malaysia, 2022*. Putrajaya: Department of Statistics Malaysia.

Department of Statistics Malaysia. (2023, July). *Current Population Estimates, Malaysia, 2023*. Putrajaya: Department of Statistic Malaysia.

Dwivedi, Y. K., Hughes, L., Baabdullah, A. M., Ribeiro-Navarrete, S., Giannakis, M., Al-Debei, M. M., Dennehy, D., Metri, B., Buhalis, D., Cheung, C. M. K., Conboy, K., Doyle, R., Dubey, R., Dutot, V., Felix, R., Goyal, D. P., Gustafsson, A., Hinsch, C., Jebabli, I., … Wamba, S. F. (2022). Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *International Journal of Information Management*, *66*, 102542. https://doi.org/10.1016/j.ijinfomgt.2022.102542

Erdfelder, E., FAul, F., Buchner, A., & Lang, A. G. (2009). Statistical power analyses using G*Power 3.1: Tests for correlation and regression analyses. *Behavior Research Methods*, *41*(4), 1149–1160. https://doi.org/10.3758/BRM.41.4.1149

Ervits, I., & Maintz, J. (2025). The trade-off between convenience and privacy: Sharing personal data with intelligent vehicles in exchange for convenient driving. *Entertainment Computing*, *54,* 100950. https://doi.org/10.1016/j.entcom.2025.100950

Fatokun, F. B., Hamid, S., Norman, A., & Fatokun, J. O. (2019). The impact of age, gender, and educational level on the cybersecurity behaviors of tertiary institution students: An empirical investigation on Malaysian universities. *Journal of Physics: Conference Series*, *1339*(1), 012098. https://doi.org/10.1088/1742-6596/1339/1/012098

Fatokun Faith, B., Hamid, S., Norman, A., Fatokun Johnson, O., & Eke, C. I. (2020). Relating factors of tertiary institution students' cybersecurity behavior. *2020 International Conference in Mathematics, Computer Engineering and Computer Science (ICMCECS 2020)*. https://doi.org/10.1109/ICMCECS47690.2020.246990

Faul, F., Erdfelder, E., Lang, A. G., & Buchner, A. (2007). G*Power 3: A flexible statistical power analysis program for the social, behavioral, and biomedical sciences. *Behavior Research Methods*, *39*(2), 175–191. https://doi.org/10.3758/BF03193146

Faul, F., Erdfelder, E., Lang, A.-G., & Buchner, A. (2009). Statistical power analyses using G*Power 3.1: Tests for correlation and regression analyses. *Behavior Research Methods*, *41*(4), 1149–1160. https://doi.org/10.3758/BRM.41.4.1149

Gillam, A. R., & Foster, W. T. (2020). Factors affecting risky cybersecurity behaviors by U.S. workers: An exploratory study. *Computers in Human Behavior*, *108*, 106319. https://doi.org/10.1016/j.chb.2020.106319

Gushelmi, Latih, R., & Zin, A. Mohd. (2024). Cybersecurity behavior in the West Sumatra universities. *International Journal on Informatics Visualization*, *8*(3–2), 1976–1986. https://doi.org/10.62527/joiv.8.3-2.3094

Hadlington, L. (2017). Human factors in cybersecurity: Examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon*, *3*(7), e00346. https://doi.org/10.1016/j.heliyon.2017.e00346

Hair Jr., J. F., Anderson, R. E., Babin, B. J., & Black, W. C. (2019). Multivariate data analysis (8th ed.). Cengage.

Hargittai, E., & Marwick, A. (2016). “What can i really do?” Explaining the privacy paradox with online apathy. *International Journal of Communication*, *10*, 3737–3757.

Hong, Y., & Furnell, S. (2021). Understanding cybersecurity behavioral habits: Insights from situational support. *Journal of Information Security and Applications*, *57*, 102710. https://doi.org/10.1016/j.jisa.2020.102710

Hyman, M. R., & Sierra, J. J. (2016). Open-versus close-ended survey questions. *Business Outlook*, *14*(2), 23–27.

Ishak, A. S., Rose, N. N., Ahmad, N., Taufiqqurahman, M., & Mustafa, M. Y. (2020). The perception and use of social media by the parent of student at University Malaysia Perlis. *Journal of Physics: Conference Series*, *1529*(2), 022001. https://doi.org/10.1088/1742-6596/1529/2/022001

Khan, N. F., Yaqoob, A., Khan, M. S., & Ikram, N. (2022). The cybersecurity behavioral research: A tertiary study. *Computers and Security, 120,* 102826. https://doi.org/10.1016/j.cose.2022.102826

Kim, B. J., & Kim, M. J. (2024). The influence of work overload on cybersecurity behavior: A moderated mediation model of psychological contract breach, burnout, and self-efficacy in AI learning such as ChatGPT. *Technology in Society*, *77,* 102543. https://doi.org/10.1016/j.techsoc.2024.102543

Koohang, A., Nord, J. H., Ooi, K. B., Tan, G. W. H., Al-Emran, M., Aw, E. C. X., Baabdullah, A. M., Buhalis, D., Cham, T. H., Dennis, C., Dutot, V., Dwivedi, Y. K., Hughes, L., Mogaji, E., Pandey, N., Phau, I., Raman, R., Sharma, A., Sigala, M., … Wong, L. W. (2023). Shaping the Metaverse into reality: A holistic multidisciplinary understanding of opportunities, challenges, and avenues for future investigation. *Journal of Computer Information Systems, 63*(3), 227–244. https://doi.org/10.1080/08874417.2023.2165197

Krejcie, R. J. & Morgan, D. W. (1970). Determining sample size for research activities. *Educational and Psychological Measurement, 30*(3), 607–610.

Kuok Tiung, L., Meri, A., Mat Nayan, L., & Othman, S. S. (2016). Uses and gratifications of news portal among Malaysian youths. *Jurnal Komunikasi: Malaysian Journal of Communication*, *32*, 790–816.

Li, L., Xu, L., & He, W. (2022). The effects of antecedents and mediating factors on cybersecurity protection behavior. *Computers in Human Behavior Reports*, *5,* 100165. https://doi.org/10.1016/j.chbr.2021.100165

Luo, J., & Ing, K. (2022). Social media and clinical Practice. In S. L. Smith & R. K. Jones (Eds.), *Mental health in a digital world* (pp. 123–135). Academic Press. https://doi.org/10.1016/B978-0-12-822201-0.00012-5

Mamade, B. K., & Dabala, D. M. (2021). Exploring the correlation between cyber security awareness, protection measures, and the state of victimhood: The case study of Ambo University's academic staffs. *Journal of Cyber Security and Mobility, 10*(4), 429–448. https://doi.org/10.13052/jcsm2245-1439.1044

Matyokurehwa, K., Rudhumbu, N., Gombiro, C., & Mlambo, C. (2021). Cybersecurity awareness in Zimbabwean universities: Perspectives from the students. *Security and Privacy, 4*(2), e141. https://doi.org/10.1002/spy2.141

Mohammad, T., Mohamed Hussin, N. A., & Husin, M. H. (2022). Online safety awareness and human factors: An application of the theory of human ecology. *Technology in Society*, *68,* 101823. https://doi.org/10.1016/j.techsoc.2021.101823

Muniandy, L., Muniandy, B., & Samsudin, Z. (2017). Cyber security behaviour among higher education students in Malaysia. *Journal of Information Assurance & Cybersecurity, 2017*, 1–10. https://doi.org/10.5171/2017.800299

Onuma, M., Kimura, A., & Mukawa, N. (2013). Exploring social cognition related to privacy settings in SNS usage. In *Proceedings of the 2013 International Conference on Signal-Image Technology and Internet-Based Systems (SITIS 2013)* (pp. 412–419). IEEE. https://doi.org/10.1109/SITIS.2013.173

Pal, P., Ghosh, S., & Kar, N. (2023). Attacks on social media networks and prevention measures. In *2023 International Conference for Advancement in Technology (ICONAT 2023)* (pp. 1–6). IEEE. https://doi.org/10.1109/ICONAT57137.2023.10080106

Patnayakuni, N., Patnayakuni, R., & Gupta, J. N. D. (2018). Towards a model of social media impacts on cybersecurity knowledge transfer: An exploration. In J. R. Smith & L. A. Brown (Eds.), *Cyber security and threats: Concepts, methodologies, tools, and applications* (pp. 480–499). IGI Global. https://doi.org/10.4018/978-1-5225-5634-3.ch028

Pollini, A., Callari, T. C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., & Guerri, D. (2022). Leveraging human factors in cybersecurity: An integrated methodological approach. *Cognition, Technology & Work, 24*(2), 335–352. https://doi.org/10.1007/s10111-021-00683-y

Prümmer, J., van Steen, T., & van den Berg, B. (2025). Assessing the effect of cybersecurity training on end-users: A meta-analysis. *Computers and Security*, *150,* 104206. https://doi.org/10.1016/j.cose.2024.104206

Raosoft. inc. (2004). *Raosoft Sample size calculator*. http://www.raosoft.com/samplesize.html.

Scala, N. M., Reilly, A. C., Goethals, P. L., & Cukier, M. (2019). Risk and the Five Hard Problems of Cybersecurity. *Risk Analysis*, *39*(10), 2031–2046. https://doi.org/10.1111/risa.13309

Shappie, A. T., Dawson, C. A., & Debb, S. M. (2020). Personality as a predictor of cybersecurity behavior. *Psychology of Popular Media*, *9*(4), 441–452. https://doi.org/10.1037/ppm0000247

Sulaiman, N. S., Fauzi, M. A., Hussain, S., & Wider, W. (2022). Cybersecurity behavior among government employees: The role of protection motivation theory and responsibility in mitigating cyberattacks. *Information, 13*(9), 0413. https://doi.org/10.3390/info13090413

Supayah, G., & Ibrahim, J. (2016). An Overview of Cyber Security in Malaysia. *Kuwait Chapter of Arabian Journal of Business and Management Review*, *6*(4), 12–20. https://doi.org/10.12816/0036698

Thompson, N., McGill, T. J., & Wang, X. (2017). "Security begins at home": Determinants of home computer and mobile device security behavior. *Computers and Security*, *70*, 348–364. https://doi.org/10.1016/j.cose.2017.07.003

Tsai, H. Y. S., Jiang, M., Alhabash, S., Larose, R., Rifon, N. J., & Cotten, S. R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. *Computers and Security*, *59,* 138–150. https://doi.org/10.1016/j.cose.2016.02.009

Tuptuk, N., & Hailes, S. (2018). Security of smart manufacturing systems. *Journal of Manufacturing Systems*, *47,* 93–103. https://doi.org/10.1016/j.jmsy.2018.04.007

Vafaei-Zadeh, A., Nikbin, D., Teoh, K. Y., & Hanifah, H. (2025). Cybersecurity awareness and fear of cyberattacks among online banking users in Malaysia. *International Journal of Bank Marketing*, *43*(3), 476–505. https://doi.org/10.1108/IJBM-03-2024-0138

Vanderkooi, D., Sangari, M. S., & Mashatan, A. (2023). Raising cybersecurity awareness through electronic word of mouth: A data-driven assessment. In *Lecture Notes in Computer Science* (Vol. 14019, pp. 398–410). Springer. https://doi.org/10.1007/978-3-031-35017-7_30

Wang, X., & Cheng, Z. (2020). Cross-sectional studies: Strengths, weaknesses, and recommendations. *Chest, 158*(1), 1346–1354. https://doi.org/10.1016/j.chest.2020.03.012

Wen, S. J., Kun, S., & Ling, T. P. (2025). Media frames and cybercrime: Understanding Malaysian online news coverage. *SEARCH: Journal of Media and Communication Research*, *2025*(Special Issue), 71–86. https://doi.org/10.58946/search-SpecialIssue.ICIMaC2024.P5

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems, 62*(1), 1–12. https://doi.org/10.1080/08874417.2020.1712269

JURNAL PENGGUNA MALAYSIA