

Analisis Elemen Niat Dalam Konsep Kepenggunaan Islam  
*Azmawida Abdullah, Mohd Murshidi Mohd Noor dan Syarifah Md Yusof*

The Factors Causing Consumers to Fall Victim to Online Shopping Scams  
*Fong Felice and Elistina Abu Bakar*

Pengetahuan, Kesedaran dan Sikap Pengguna Terhadap Amalan Kitar Semula Dalam  
Norma Baharu di Arau, Perlis  
*Nuridayu Abdul Rahim dan Zuroni Md Jusoh*

Factors Influencing the Usage Behaviour of E-Wallets among Undergraduates in  
Klang Valley  
*Lee Mei Kei and Syuhaily Osman*

Analisis Faktor-Faktor yang Mempengaruhi Niat Pembelian Produk Hiliran Kelapa Sawit  
di Malaysia  
*Mohd Ikram Bin Mohamad @ Yusof, Lai Wei Sieng dan Mustazar Mansur*

Determinants of Petrol Station Employees Safety Practices  
*Ariff Azril Faridzuan Teo and Afida Mastura Muhammad Arif*

Modern Media Era on Social Media Consumer Purchase Decision of Beauty Products  
*Rozita Naina Mohamed, Zuroni Md Jusoh, Husna Nisa Mohd Nizam and Habib Mazlan*

The Impact of Covid-19 on Customer Buying Behaviour: A Study on Gen Z in  
Universiti Utara Malaysia (UUM)  
*Nurin Aina Akmal Abdul Malik, Normalisa Md Isa, Norkhazzaina Salahuddin and  
Amr Mohammed Nasser Al-ganad*

The Role of the Education System in Influencing the Terengganu Graduate Job Market  
*Anis Mat Dalam, Muhammad Imran Sofi Mahmuddin and Noorhaslinda Kulub Abd Rashid*

Credit Attitude, Money Attitude and Credit Misuse among University Students in China  
*Wen Tao, Koa and Jasmine Leby, Lau*

# JURNAL PENGGUNA MALAYSIA

---

## Lembaga Pengarang

Zuroni Md Jusoh (Dr.) (Ketua Editor)	Fakulti Ekologi Manusia, Universiti Putra Malaysia
Syuhaily Osman (Prof. Madya Dr.)	Fakulti Ekologi Manusia, Universiti Putra Malaysia
Elistina Abu Bakar (Prof. Madya Dr.)	Fakulti Ekologi Manusia, Universiti Putra Malaysia
Afida Mastura Muhammad Arif (Prof. Madya Dr.)	Fakulti Ekologi Manusia, Universiti Putra Malaysia
Rozita Naina Mohamed (Prof. Madya Dr.)	Fakulti Pengurusan dan Perniagaan, Universiti Teknologi MARA
Nur Jasmine Lau Leby (Dr.)	Fakulti Ekologi Manusia, Universiti Putra Malaysia
Siti Yuliandi Ahmad (Dr.)	Kulliyah of Languages and Management, Universiti Islam Antarabangsa Malaysia
Monizaihasra Mohamed (Dr.)	Fakulti Perniagaan Ekonomi dan Pembangunan Sosial, Universiti Malaysia Terengganu
Normalisa Md Isa (Dr.)	Pusat Pengajian Pengurusan Perniagaan Kolej Perniagaan, Universiti Utara Malaysia
Megawati Simanjuntak (Dr.)	Fakultas Ekologi Manusia, Institut Pertanian Bogor, Indonesia
Gancar Candra Premananto (Prof. Madya Dr.)	Fakultas Ekonomi dan Bisnis, Universitas Airlangga, Indonesia

---

JURNAL PENGGUNA MALAYSIA adalah keluaran Persatuan Ekonomi Pengguna dan Keluarga Malaysia. Ia bertujuan untuk menyebarkan, menambah dan berkongsi maklumat berkaitan hal ehwa, 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

Analisis Elemen Niat Dalam Konsep Kepenggunaan Islam <i>Azmawida Abdullah, Mohd Murshidi Mohd Noor dan Syarifah Md Yusof</i>	1
The Factors Causing Consumers to Fall Victim to Online Shopping Scams <i>Fong Felice and Elistina Abu Bakar</i>	17
Pengetahuan, Kesedaran dan Sikap Pengguna Terhadap Amalan Kitar Semula Dalam Norma Baharu di Arau, Perlis <i>Nuridayu Abdul Rahim dan Zuroni Md Jusoh</i>	30
Factors Influencing the Usage Behaviour of E-Wallets among Undergraduates in Klang Valley <i>Lee Mei Kei and Syuhaily Osman</i>	55
Analisis Faktor-Faktor yang Mempengaruhi Niat Pembelian Produk Hiliran Kelapa Sawit di Malaysia <i>Mohd Ikram Bin Mohamad @ Yusof, Lai Wei Sieng dan Mustazar Mansur</i>	75
Determinants of Petrol Station Employees Safety Practices <i>Ariff Azril Faridzuan Teo and Afida Mastura Muhammad Arif</i>	96
Modern Media Era on Social Media Consumer Purchase Decision of Beauty Products <i>Rozita Naina Mohamed, Zuroni Md Jusoh, Husna Nisa Mohd Nizam and Habib Mazlan</i>	109
The Impact of Covid-19 on Customer Buying Behaviour: A Study on Gen Z in Universiti Utara Malaysia (UUM) <i>Nurin Aina Akmal Abdul Malik, Normalisa Md Isa, Norkhazzaina Salahuddin and Amr Mohammed Nasser Al-ganad</i>	124
The Role of the Education System in Influencing the Terengganu Graduate Job Market <i>Anis Mat Dalam, Muhammad Imran Sofi Mahmuddin and Noorhaslinda Kulub Abd Rashid</i>	143
Credit Attitude, Money Attitude and Credit Misuse among University Students in China <i>Wen Tao, Kao and Jasmine Leby, Lau</i>	164

---

## PENYUMBANG ARTIKEL

---

Afida Mastura Muhammad Arif	Fakulti Ekologi Manusia, Universiti Putra Malaysia
Amr Mohammed Nasser Al-ganad	School of Business Management, Universiti Utara Malaysia
Anis Mat Dalam	Faculty of Business, Economics, and Social Development Universiti Malaysia Terengganu
Ariff Azril Faridzuan Teo	Fakulti Ekologi Manusia, Universiti Putra Malaysia
Azmawida Abdullah	Islamic Business School, Universiti Utara Malaysia
Elistina Abu Bakar	Fakulti Ekologi Manusia, Universiti Putra Malaysia
Fong Felice	Fakulti Ekologi Manusia, Universiti Putra Malaysia
Habib Mazlan	Fakulti Ekologi Manusia, Universiti Putra Malaysia
Husna Nisa Mohd Nizam	Fakulti Ekologi Manusia, Universiti Putra Malaysia
Jasmine Leby, Lau	Fakulti Ekologi Manusia, Universiti Putra Malaysia
Lai Wei Sieng	Fakulti Ekonomi & Pengurusan, Universiti Kebangsaan Malaysia
Lee Mei Kei	Fakulti Ekologi Manusia, Universiti Putra Malaysia
Mohd Ikram Bin Mohamad @ Yusof	Fakulti Ekonomi & Pengurusan, Universiti Kebangsaan Malaysia
Mohd Murshidi Mohd Noor	Islamic Business School, Universiti Utara Malaysia
Muhammad Imran Sofi Mahmuddin	Faculty of Business, Economics, and Social Development Universiti Malaysia Terengganu
Mustazar Mansur	Fakulti Ekonomi & Pengurusan, Universiti Kebangsaan Malaysia
Noorhaslinda Kulub Abd Rashid	Faculty of Business, Economics, and Social Development Universiti Malaysia Terengganu
Norkhazzaina Salahuddin	School of Business Management, Universiti Utara Malaysia
Normalisa Md Isa	School of Business Management, Universiti Utara Malaysia
Nuridayu Abdul Rahim	Fakulti Ekologi Manusia, Universiti Putra Malaysia
Nurin Aina Akmal Abdul Malik	Othman Yeop Abdullah Graduate School of Business (OYAGSB), Universiti Utara Malaysia
Rozita Naina Mohamed	Faculty of Business & Management, Universiti Teknologi MARA
Syarifah Md Yusof	Islamic Business School, Universiti Utara Malaysia
Syuhaily Osman	Fakulti Ekologi Manusia, Universiti Putra Malaysia
Wen Tao, Koa	Kumpulan Penyelidikan Penggunaan Lestari, Fakulti Ekologi Manusia, Universiti Putra Malaysia
Zuroni Md. Jusoh	Fakulti Ekologi Manusia, Universiti Putra Malaysia
	Kumpulan Penyelidikan Penggunaan Lestari, Fakulti Ekologi Manusia, Universiti Putra Malaysia

---

# THE FACTORS CAUSING CONSUMERS TO FALL VICTIM TO ONLINE SHOPPING SCAMS

Fong Felice<sup>1</sup>  
Elistina Abu Bakar<sup>1</sup>

Corresponding author: Elistina Abu Bakar (email: elistina@upm.edu.my)

## Abstract

This study aimed to identify the factors that contribute to the behaviours of potential victims of online shopping scams. One hundred fifty respondents who participated in this study were chosen using the multistage random sampling method. Data were collected using a set of questionnaires to identify threat awareness, technological advancement, negative emotions, and consumers' online behaviours. The self-control theory was adopted to explain the behaviours of consumers and their factors. The findings showed a significant relationship between all three independent variables (threat awareness, technological advancement, and negative emotion) with the dependent variable (the behaviour of online shopping scam victims). The findings from this study would help the consumer groups or government increase the awareness among online shopping consumers so that they will not fall for scams easily. Other than that, by knowing the factors contributing to the behaviours of potential victims of online shopping scams, consumers will be more alert and will not perform impulsive purchasing without further consideration.

**Keywords:** Online scams; Consumers' behaviours; Awareness; Technology; and Emotion.

## Abstrak

*Kajian ini bertujuan untuk mengenal pasti faktor-faktor yang menyumbang kepada tingkah laku mereka yang berpotensi untuk menjadi mangsa penipuan membeli-belah dalam talian. Seratus lima puluh orang responden yang mengambil bahagian dalam kajian ini dipilih menggunakan kaedah persampelan rawak peringkat. Data dikumpul menggunakan satu set soal selidik untuk mengenal pasti kesedaran terhadap ancaman, kemajuan teknologi, negatif emosi dan tingkah laku dalam talian pengguna. Teori Kawalan Kendiri telah diterima pakai untuk menerangkan tingkah laku pengguna dan faktornya. Penemuan menunjukkan hubungan yang signifikan antara ketiga-tiga pembolehubah tidak bersandar (kesedaran terhadap ancaman, kemajuan teknologi, dan negatif emosi) dengan pembolehubah bersandar (tingkah laku mangsa penipuan membeli-belah dalam talian). Dapatan daripada kajian ini*

---

<sup>1</sup>Department of Resource Management and Consumer Studies, Faculty of Human Ecology, Universiti Putra Malaysia

*akan membantu kumpulan pengguna dan kerajaan untuk meningkatkan kesedaran dalam kalangan pengguna dalam talian supaya mereka tidak mudah terjebak dengan penipuan. Selain itu, dengan mengetahui faktor-faktor yang menyumbang kepada tingkah laku bakal mangsa penipuan membeli-belah dalam talian, pengguna akan lebih berwaspada dan tidak akan melakukan pembelian impulsif tanpa pertimbangan lanjut*

**Kata kunci:** *Penipuan dalam talian; Tingkah laku pengguna; Kesedaran; Teknologi dan Emosi.*

## **Introduction**

The internet has become one of the daily needs of consumers as it brings many benefits to consumers, including saving time and energy, enhancing long-distance relationships, easy ways to access information, and so on. Today, we live in a networked society with cloud computing, online transaction, and other interactions made possible by Internet technology (Phillips & Wilder, 2020). It stated clearly that the Internet had become very general among consumers. However, the rapid growth of the Internet and the advance in technology have brought risks for consumers whereby they have the chance to be the victims of online scams.

Online scams can be defined as a crime in which the perpetrator develops a scheme using one or more elements of the internet to deprive a person and get benefits from the targeted person. Scams are described as misleading actions to obtain information or money. On a large scale, end users are deceived, and impersonation is used to get a target's information (Sanchez, Torress, Zambrano & Flores, 2018; Bailey et al., 2021). Online scams differ from online frauds as the latter is a broader category of wrongdoing than a scam, meaning that a scam is a subordinate category of fraud.

Usually, the scam involves money, while fraud may or may not. Victims of scams can suffer significant financial and psychological distress (Martens, Wolf & Marez, 2019; Aneke et al. (2020). Scams are committed by e-mail, telephone, text messages, or social media. According to the Australian Competition & Consumer Commission (ACCC), it concluded that the most common types of online scams are the attempt to gain an individual's personal information, buying or selling products and services, dating and romance, fake charities, investments, jobs and employment, threats and extortion, unexpected money as well as unexpected winnings. After the COVID-19 outbreak, the cases of online shopping scams kept increasing, and new types of scams appeared, including online face mask scams, immunization scams, fraudulent sales of PPE, etc. Scammers will tend to grab consumers' attention by offering a lower price. During the outbreak of COVID-19, the cost of face masks and hand sanitiser rose drastically, which made some consumers fall into the trap. Criminals

offer fake products at meagre prices and provide fake positive consumer comments to attract victims (Octasia, 2018; Zahari et al., 2019).

News related to online scams never stopped, reminding consumers that the risk of becoming victims of online scams still exists. According to a statement from PDRM's Commercial Crime Department, 4,764 Macau scam cases involving a total loss of over RM232 million happened between January and September 2020. In Malaysia and Singapore, scam cases also faced an increase. According to Channel News Asia (CAN) sources, 9,502 scams were reported in 2019, compared to 6,189 cases reported in the previous year. Based on the statistics released by the Ministry of Domestic Trade and Consumer Affairs (MDTCA), online shopping scams had become uncontrollable during the Movement Control Order (MCO) during March and June 2020, whereby there were 24,018 cases of online shopping scams reported (Borneopost, 2022). Due to the increasing number of people shopping online, Malaysians lose an average of RM100,000 daily to online scammers (Hoh, 2020).

Most consumers are familiar with the term 'online shopping scams.' However, why do consumers still become a victim of it? Many factors drive consumers to fall for online scams and become the victims who lose their money; even worse is the love scams that might destroy the victim's life. Therefore, this paper investigates a few factors to see the relationship between them and online shoppers' behaviour. The factors are threat awareness, technological advancement, and negative emotions.

## **Literature Review**

Self-control theory was initially developed to explain the determinants of offending behaviour (Gottfredson & Hirschi, 1990). The self-control theory of crime declares that individuals with low self-control have a more significant tendency to involve themselves in any criminal. This scenario is defined as "acts of force or fraud undertaken to pursue self-interest" (Gottfredson & Hirschi, 1990). Morris (2019) stated that self-control theory is one of the leading models in criminology. This theory presumes that all individuals are self-interested, and there will be a possibility for them to commit a crime when an opportunity appears (Back, Soor & LaPrade, 2018). Persons with low self-control are impulsive, insensitive, action-oriented, negatively tempered, and risk-takers who tend to perform poorly and fail to meet the responsibilities of school, work, and family (Gottfredson & Hirschi, 1990). This theory is adopted to see the factors that lead a person to behave in such a way and subsequently fall into the traps of a wicked person trying to take undue advantage of this person. Among the factors is less control within the individual due to internal (awareness and emotion) or external influences (technological advances).

## Threat Awareness

The threat is an impulsivity component of the self-control theory. A threat is a statement of an intention to inflict pain, injury, damage, or other hostile action on someone in retribution for something done or not done. At the same time, awareness is knowledge or perception of a situation or fact. Therefore, threat awareness can be defined as knowing about an action or intention that might bring harm or damage. Threat awareness plays a prominent role because consumers can be more alert as they learn about how the scams occur and the possible consequences once they become victims of an online scam. Some consumers are only partially aware or have little basic knowledge about online scams. Participants (refers to consumers) understood that people's details were passed between fraudsters but had little or no understanding of how the fraud against them had been committed (Button et al., 2014).

According to McAlpine (2016), threat awareness determines the systems, facilities, and utilization considered essential to an organization, making the controls and protections needed to fix a problem. He also stated that threat awareness consists of having a plan and being alert to the threat when the individuals are aware of it. From the view of online fraud and cybercrimes, threat awareness focuses on knowing what threat exists (Hanus & Wu, 2016). Siponen, Pahlila & Mahmood (2006) suggested that threat awareness influences the rationale behind the motivation to defend against cybercrime. Hanus & Wu (2016) also mentioned that individuals with higher levels of threat awareness could build up their protective reactions and bring their risky responses towards information security threats to the minimum level. Thus, the following hypothesis was formulated;

H<sub>0</sub>1: There is no significant relationship between threat awareness and the behaviour of potential victims of online shopping scams.

## Technological Advancement

Technological advancement is a risk-seeking component of the self-control theory. Technological advancement is merging and using knowledge to develop new ideas (Imran, Maqbool & Shafique, 2014). Schwab (2016) described technological advances as a 'revolution' due to their 'velocity, scope, and system impact.' The advance in technology offers a chance for online scammers to execute their plans as online provides them with a broader platform; in another saying, online gives them more potential victims (Phillips, & Wilder, 2020). In this modern generation, most business transactions have been shifted online to enjoy E-commerce benefits. Consequently, the scam has followed as perpetrators update old scams for a digital age and develop new ones (Hamsi, Bahry, Toby & Masrom, 2015). The anonymous



online environment makes it difficult for users to identify such fraudulent probes (Bay, Cook, Grubisic, & Nikitkov, 2014). Thus, the following hypothesis was formulated;

H<sub>0</sub>2: There is no significant relationship between technological advancement and the behaviour of potential victims of online shopping scams.

## **Negative Emotion**

Negative emotion is within the temper component in the self-control theory. Pam (2013) defined negative emotion as an unpleasant emotion felt by an individual that negatively affects the person. Negative emotionality is more likely to be linked with anger and fears. Other than that, Young, Sandman, & Craske (2019) stated that some scholars agreed that negative emotions also included depression, anxiety, and stress. Isen, Shalke, Clark, & Karp (1978) said that individuals experiencing negative emotional states are also likely to focus on achieving a short-term goal to release their tension in a shorter period. It will make them particularly vulnerable. This opinion was also supported by Ferdrickson & Branigan (2005), who stated that people would have a more significant possibility of being involved in the failure of self-control and have a narrow focus of attention when they are feeling distressed. As such, negative emotions will lead to negative consequences. Arslan et al. (2019) associated negative emotions with cyberbullying. Lu et al. (2020) also emphasized managing emotion to curb scams. Norris & Brookes (2021) also found that emotion leads to how people perceive online scams. Thus, the following hypothesis was formulated;

H<sub>0</sub>3: There is no significant relationship between negative emotion and the behaviour of potential victims of online shopping scams.

## **Research Methodology**

The location chosen by the researchers is Kampar, Perak, after applying random sampling. The researchers listed down the districts in Perak and picked one randomly. The selection for the district was repeated through the same process as the selection of the residential areas. The researchers picked house numbers randomly and made a short visit to the selected houses. The visited families were invited to be the respondents of this study, and once they agreed, the google form would be given. According to Roscoe (1975), a sample size with a range larger than 30 and less than 500 respondents is appropriate for most research. Hence, the sample size for this study is 150 respondents would be adequate for an exploratory study.

The google form questionnaire consists of four sections, including respondents' demographic profile, threat awareness, technological advancement, negative emotion, and behaviour. The respondents were required to answer the questionnaire

based on Five-point Likert Scale ranging from 1=Strongly Disagree to 5=Strongly Agree. A five-point Likert scale was employed to reduce respondents' frustration and increase response rate and quality.

Items in threat awareness, technological advancement, and negative emotions were all adopted by Grasmick et al. (1993), Arneklev et al. (1993), and Padil et al. (2020). On the other hand, the items of the potential behaviour of scam victims were self-developed. In this study, Pearson correlation has been used to test the correlation between the independent variables and the dependent variable. The reliability test score for threat awareness was 0.875, technological advancement was 0.742, negative emotions 0.858, and behaviour was 0.9. The items were reliable and can be used for further analysis.

## **Findings and Discussion**

### **Background of the Respondents**

Table 1 presented the demographic profile of the respondents, which involved gender, age group, race, educational level, and how frequently the respondents purchase online. Of the 150 respondents, 88 female respondents represented 58.7%, and 62 male respondents represented 41.3%. This showed that more female respondents participated in this study than male respondents. For the age group, Generation Y had the highest frequency and percentage, which was 42.7% (64 respondents), followed by Generation Z with 41.3% (62 respondents), and the least was Generation X with 16% (24 respondents). Among 150 respondents, the Chinese had the highest frequency and percentage, 56% (84 respondents). It was followed by Malay, which comprised 28.7% (43 respondents) of the total respondents. Next, Indians recorded 11.3% (17 respondents), and the least was other races, with only 4% (6 respondents). Most respondents were undergraduate students based on the data collected, with 44% (66 respondents) from 150 respondents. Next, it continued with respondents with a diploma whereby had 27.3% (41 respondents), followed by respondents with the Malaysian Higher School of Certificate (STPM) with 20.7% (31 respondents).

The option of one to three times within a week had the highest percentage, which was 68.7% (103 respondents). It was followed by the second option, four to six times within a week; it had 29.3% (44 respondents). Last but not least, 2% (3 respondents) chose to purchase online seven to nine times within a week. There were no respondents from the fourth option to purchase online ten times or above within a week.

**Table 1: Demographic Profile of Respondents**

	Frequency (n)	Percentage (%)
<b>Gender</b>		
Male	62	41.3
Female	88	58.7
<b>Age Group</b>		
Generation X	24	16.0
Generation Y	64	42.7
Generation Z	62	41.3
<b>Race</b>		
Chinese	84	56.0
Malay	43	28.7
Indian	17	11.3
Other	6	4.0
<b>Educational Level</b>		
PMR/SRP	10	6.7
SPM	-	-
STPM	31	20.7
Diploma	41	27.3
Degree	66	44
Master	2	1.3

**Consumers’ Behaviour**

Six statements with a five-point Likert scale, represented by options 1 to 5, stand for strongly disagree to strongly agree to measure the behaviours of potential victims of online shopping scams. Table 2 shows the score of means and standard deviation for each statement.

**Table 2: Behaviour of Potential Victims of Online Shopping Scams**

No	Statement	Mean	SD
1.	I do not search for information about online sellers before I go online.	3.64	1.43
2.	I do not like to stop and think over before making a purchasing decision.	3.88	1.28
3.	I am not a cautious person when it comes to online shopping.	3.86	1.23
4.	I seldom think carefully before purchasing from an online store.	3.95	1.22
5.	Before making up my mind, I will not consider all the risks of online shopping.	3.87	1.25
6.	I do not read the reviews by other consumers about the items that I want to purchase from an online store.	3.16	1.47

The statement with the highest mean score was 'I seldom think carefully before purchasing from an online store.' It indicated that negative behaviour and buying without thinking would lead to online scams. This group of consumers quickly falls victim since unscrupulous traders can easily deceive them. Other statements also show a mean score above three, which can be considered high. The higher the mean score, the more negative the behaviour is. The behaviour of potential victims of online shopping scams had a mean score of 3.73, slightly higher than the neutral value. It showed that the respondents had some of the behaviour listed, such as not being cautious while purchasing online and not reading the review, making them potential victims of online shopping scams.

### ***Relationship Between Threat Awareness, Technological Advancement, Negative Emotions, and Consumers' Behaviour***

According to Table 3, the Pearson Correlation Coefficient (R-value) for threat awareness was 0.67, which meant that it had a moderate relationship with the behaviour of potential victims of online shopping scams. In this study, threat awareness can be referred to as the extent to which consumers are alerted of online shopping scams and how deep their understanding of them is. The listed statements were negative phrases; hence, this study's high threat awareness score meant that the respondents lacked knowledge of online shopping scams and were not beware of them. Other than that, the p-value of the correlation between threat awareness and the behaviour of potential victims of online shopping scams was .000. Hence, a significant relationship existed between threat awareness and the behaviour of potential victims of online shopping scams. Therefore,  $H_{01}$  was rejected.

The technological advancement scored an R-value of 0.24, and the correlation coefficient of 0.24 indicated a weak correlation between technological advancement and the behaviour of potential victims of online shopping scams. Technological advancement in this study can be referred to as the advantages of the technology that might make a consumer fall victim to online shopping scams. A weak correlation coefficient existed, but the p-value was significant. It was clear that technological advancement had a substantial relationship with the behaviour of potential victims of online shopping scams. Therefore,  $H_{02}$  was rejected.

Table 3 shows the Pearson Correlation Coefficient (R-value) for negative emotion, and the behaviour of potential victims of online shopping scams was 0.75. The score of 0.75 indicated a strong correlation between the two involved variables. In this study, negative emotion was more likely to describe the bad feelings of respondents, such as anger and sadness. When the negative emotion scores are higher, most respondents will potentially fall for online scams. Hence,  $H_{03}$  was also rejected.

**Table 3: Results of Pearson Correlation Coefficient Test**

	(R-value)	Significance (p-value)
Threat Awareness	.670***	.000
Technological Advancement	.243***	.003
Negative Emotion	.747***	.000

Note: \*Significant at  $p \leq 0.05$

The previous findings by Rajan (2013) stated that there are possibilities to fall for mobile phone scams if the users use gadgets and perform online shopping without awareness. Moreover, the research findings in Nigeria by Aneke et al. (2020) found that Internet technology has created a new form of criminality, and cybercrime is significantly related to the technology. According to Bailey et al. (2021), everyone is a potential victim of cybercrime with the advances in technology, phones, and internet-enabled services. Button et al. (2014) found that technological advancements are growing speedily, which means the development of cybercrime is the same. Other than that, Lacey, Goode, Pawada & Gibson (2020) also stated that many cybercrime cases went up due to the continuous effects of the Internet. It was noted that cybercrime is a product of advances in Internet technology. Other than that, research done by Norris, Brookes & Dowell (2019) and Lu et al. (2020) also stated that mood, which means emotion, could be one key factor influencing how we process potentially fraudulent communications. All three independent variables were generated from the self-control theory. Louderback & Antonaccio (2020) found that individual characteristics such as awareness and emotion were significantly related to fraud crime. Hence, the result was supported by the previous studies.

## Implications and Conclusion

In this study, the three variables (threat awareness, technological advancement, and negative emotion) were found to have a significant relationship with the behaviour of potential victims of online shopping scams. Hence, it is crucial to take some actions to ensure that consumers will not fall for online shopping scams easily. The actions taken are advised to use the variables listed as a guideline since significant relationships were found. For threat awareness, it is vital to increase awareness among consumers. They need to know more about online shopping scams and the tricks that online scammers might use to make consumers fall for scams. It is undeniable that online shopping brings many conveniences, but the potential risk lies there simultaneously. Related authorities, such as governments and consumer groups, can organize campaigns that can help in increasing awareness among consumers. Some consumers might know about online shopping scams but do not know about the latest type of scam. Hence, organizing awareness campaigns can educate consumers who have no idea about online shopping scams will learn about

it. While for those who know about online shopping scams but still lack the latest information, they will get to know them in detail after joining the campaigns. Threat awareness needs to be explained. Convenience is provided by online shopping, but there are still some threats, such as accidentally being the victim of an online shopping scam. Hence, it is crucial to introduce the perils of online shopping scams and increase awareness.

Technological advancement is also one of the factors of people falling into the victimization of online shopping scams. In this case, consumers are suggested to use mobile phones with a better security system. Scammers can also quickly obtain consumers' contact numbers due to technological advances. Hence, consumers should not answer the calls that strangers make. Besides, the findings also showed a significant relationship between negative emotion and the behaviour of potential victims of online shopping scams. Negative emotion must be handled carefully because negative emotion can lead to many criminal cases. Consumers should be more alert when they have negative feelings. Consumers should not make impulsive purchases without listening to other people's opinions. When negative emotions exist within a consumer, consumers are advised to calm down and reason instead of holding a mobile phone. Consumers are advised not to do impulsive purchasing because limited time is used to make a purchasing decision; it is too risky and probably will lead to an online shopping scam. Highlighting the potential factors and presenting the final results will help consumers understand online shopping scams. It will make consumers more alert and careful while performing online shopping.

## References

- Aneke, S. O., Udanor, C., Nweke, O. & Ogbodo, I. A. (2020). Towards determining cybercrime technology evolution in Nigeria. *International Journal of Latest Technology in Engineering, Management & Applied Science (IJLTEMAS)*, IX (IV), 27-43.
- Arneklev, B. J., Grasmick, H. G., Tittle, C. R. & Bursik, Jr. R. J. (1993). Low self-control and imprudent behaviour. *Journal of Quantitative Criminology*, 9 (3),5-29.
- Arslan, P., Corazza, M., Cabrio, E., & Villata, S. (2019). Overwhelmed by negative emotions? Maybe you are being cyber-bullied! SAC 2019 - The 34th ACM/SIGAPP Symposium on Applied Computing, Limassol, Cyprus.
- Back, S., Soor, S. & LaPrade, J. (2018). Juvenile hackers: an empirical test of self-control theory and social bonding theory. *International Journal of Cybersecurity Intelligence & Cybercrime*, 1 (1), 40-55.

- Bailey, J., Taylor, L., Kingston, P., & Watts, G. (2021). Older adults and “scams” evidence from the mass observation archive. *The Journal of Adult Protection*, 23(1), 57-69.
- Bay, D., Cook, G.L., Grubisic, J., & Nikitkov, A. (2014). Identifying fraud in online auctions: A case study. *Accounting Perspective*, 13 (4), 283-299.
- Borneopost (March 15, 2022). KPDNHEP: 24,018 complaints on online fraud and electronic scams during a pandemic. Retrieved from <https://www.theborneopost.com/2022/03/15/kpdnhep-24018-complaints-on-online-fraud-electronic-scams-during-pandemic/>.
- Button, M., Nicholls, C. M., Kerr, J., & Owen, R. (2014). Online frauds: learning from victims why they fall for these scams. *Australian & New Zealand Journal of Criminology*, 47(3), 391-408.
- Button, M., Nicholls, C. M., Kerr, J., & Owen, R. (2015). Online fraud victims in England and Wales: victims' views on sentencing and the opportunity for restorative justice. *The Howard Journal*, 54 (2), 193-211.
- Ferdrickson, B.L. & Branigan, C. (2005), Positive emotions broaden the scope of attention and thought-action repertoires. *Cognition & Emotion*, 19 (3), 313-332.
- Gottfredson, M. R. & Hirschi, T. (1990). *A general theory of crime*. Stanford University Press.
- Grasmick, H. G., Tittle, C. R., Bursik Jr, R. J., & Arneklev, B. J. (1993). Testing the core empirical implications of Gottfredson and Hirschi's general theory of crime. *Journal of Research in Crime and Delinquency*, 30(1), 5-29.
- Hamsi, A. S., Bahry, F. D. S., Tobi, S. N. M., & Masrom, M. (2015). Cybercrime over internet love scams in Malaysia: a discussion on the theoretical perspectives, connecting factors, and keys to the problem. *Journal of Management Research*, 7(2), 169.
- Hanus, B & Wu, Y.A (2016) Impact of users' security awareness on desktop security behavior: A protection motivation theory perspective. *Information Systems Management*, 33 (1), 2-16.
- Hoh, K. S. (2020). Malaysians lose RM100,000 a day to online shopping cheats. Retrieved from <https://www.thesundaily.my/local/malaysians-lose-rm100000-a-day-to-online-shopping-cheats-LJ5847951>

- Imran, M., Maqbool, N., & Shafique, H. (2014). Impact of technological advancement on employee performance in banking sector. *International Journal of Human Resource Studies*, 4(1), 2162-3058.
- Izen, A. M., Shalke, T. E., Clark, M., & Karp, L. (1978). Affect, accessibility of material in memory, and behavior: A cognitive loop? *Journal of Personality and Social Psychology*, 36(1), 1-12.
- Lacey, D., Goode, S., Pawada, J., & Gibson, D. (2020). The application of scam compliance models to investment fraud offending. *Journal of Criminological Research, Policy, and Practice*, 6 (1), 65-81.
- Louderback, E. R. & Antonaccio, O. (2020). New applications of self-control theory to computer-focused cyber deviance and victimization: a comparison of cognitive and behavioral measures of self-control and test of peer cyber deviance and gender as moderators. *Crime & Delinquency*, 67(3), 366-398.
- Lu, H.Y., Chan, S., Chai, W., Lau, S. M., & Khader, M. (2020). Examining the influence of emotional arousal and scam preventive messaging on susceptibility to scams. *Crime Prevention Community Safety*, 22(4), 313–330.
- Martens, M., Wolf, R. D., & Marez, L. D. (2019). Investigating and comparing the predictors of the intention towards taking security measures against malware, scams, and cybercrime in general. *Computers in Human Behaviour*, 92, 139-150.
- McAlpine, K. (2016). How threat awareness is different from threat intelligence. Retrieved from <https://www.securityweek.com/how-threat-awareness-different-threat-intelligence>.
- Morris, R. C. (2019). Self-control as a criminogenic need: a longitudinal test of social intervention to improve self-control. *Criminology, Criminal Justice, Law & Society*, 20 (1), 13-34.
- Norris, G. & Brookes, A. (2021). Personality, emotion and individual differences in response to online fraud. *Personality and Individual Differences*, 169, 109847.
- Octasia, D. Y. (2018). The effect of convenience and security on users' trust and satisfaction of E-commerce in Indonesia (study on customers of TOKOPEDIA in Jabodetabek region). *Journal of Information Engineering and Applications*, 8 (4), 1-5.



- Padil et al., (2020). An exploratory factor analysis of financial literacy and awareness of investment scams. *International Invention, Innovative & Creative (InIIC) Conference*, Series 2/2020.
- Pam, M. S., (2013). Negative emotion. Retrieved from <https://psychologydictionary.org/negative-emotion/>
- Phillips et al., (2020). Tracing cryptocurrency scams: clustering replicated advance-fee and phishing websites, *2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, pp. 1-8.
- Rajan, A. P. (2013). A study on security threat awareness among students using social networking sites by applying data mining techniques. *International Journal of Research in Commerce, IT & Management*, 3(9), 2231-5756.
- Roscoe, A. M., Lang, D., & Sheth, J. N. (1975). Follow-up methods, questionnaire length, and market differences in mail surveys: In this experimental test, a telephone reminder produced the best response rate and questionnaire length had no effect on rate of return. *Journal of Marketing*, 39(2), 20-27.
- Sánchez et al., (2018). FraudFind: Financial fraud detection by analyzing human behavior, *IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC)*, 281-286.
- Schwab, K. (2017) The Fourth Industrial Revolution. World Economic Forum. Retrieved from [https://www.scirp.org/\(S\(lz5mqp453edsnp55rrgjct55\)\)/reference/ReferencesPapers.aspx?ReferenceID=2019783](https://www.scirp.org/(S(lz5mqp453edsnp55rrgjct55))/reference/ReferencesPapers.aspx?ReferenceID=2019783).
- Siponen et al., (2006). Factors influencing protection motivation and security policy compliance. *Innovations in Information Technology*, 1-5
- Young, K.S., Sandman, C.F., & Craske, M.G. (2019). Positive and negative emotion regulation in adolescence: links to anxiety and depression. *Brain Sci.*, 9, 76
- Zahari, et al (2019). The role of familiarity, trust and awareness towards online fraud. *Journal of Research and Opinion*, 6(9), 2470-2480.

Jurnal  
Pengguna Malaysia

ISSN 1511-998X

