Journal of Ecohumanism
2024
Volume: 3, No: 3, pp. 1626– 1638
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i3.3327

Small Steps, Big Security: TAM-Powered Insights of Cybersecurity Adoption among Small-and-Medium Entrepreneurs in Digital Business

Nur Raidah Radzi[1], Siti Nor Amalina Ahmad Tajuddin[2*], Khairul Azam Bahari[3]

Abstract

Embracing digital business enhances company resilience, yet small and medium-sized enterprises (SMEs) often lack resources to combat cyber threats, unlike larger enterprises. Sophisticated cyberattacks surpass standard antivirus software, necessitating a shift in cybersecurity strategies. Therefore, this study aimed to investigate the relationship between knowledge, perceived usefulness, perceived ease of use, and the adoption of cybersecurity among small-and-medium entrepreneurs in Perak, Malaysia. Guided by the Technology Acceptance Model (TAM), this ongoing research employed a quantitative approach by distributing questionnaires to 400 digital entrepreneurs in the small and medium-sized business sectors in Perak. The findings revealed that the majority of entrepreneurs possessed a relatively high level of knowledge about cybersecurity. Furthermore, the study identified a strong positive correlation between knowledge and perceived usefulness (correlation coefficient r = 0.639), as well as a moderately positive correlation between knowledge and perceived ease of use (correlation coefficient r = 0.435) among small and medium entrepreneurs in Perak. Consequently, this study contributes to a better understanding of the Technology Acceptance Model (TAM) within the context of perceived usefulness, perceived ease of use, and the adoption of cybersecurity, thereby enriching the existing literature on cybersecurity among small and medium entrepreneurs in the era of digital business.

Keywords: *Cybersecurity, Digital Business, Small-and-medium entrepreneurs, Technology acceptance model (TAM).*

Introduction

In recent years, the global landscape of cybersecurity has become increasingly complex as numerous enterprises gear up to transition their operations towards the digital marketing. This transformation has gained significant momentum due to the impact of the Covid-19 pandemic, driving more marketing activities onto digital platforms. Consequently, the escalation of cybersecurity threats, risks, and challenges, especially for small and medium-sized enterprises (SMEs), has become a pressing concern (Fernandez De Arroyabe & Fernandez de Arroyabe, 2023). Past research indicates that small and medium-sized enterprises (SMEs) tend to downplay their susceptibility to cyberattacks, even when they have some awareness of the associated risks. However, these assessments of vulnerability typically rely on a broad understanding of cyber threats rather than being linked to specific and commonly encountered types of threats (Wilson et al., 2023). Given the economic impact of cybersecurity incidents and the frequency with which businesses are targeted by cyber threats, it is vital for SMEs to adopt cybersecurity measures to secure their survival in the case of an attack (Wilson et al., 2023). Small businesses, particularly those with 1-49 employees, face an average annual loss of approximately US$14,000 per firm in the United States and certain European countries (Tam et al., 2021). Although data for small businesses is limited, a US Government report suggests that the impact and cost of a cyber breach on small businesses could be more severe than on larger businesses, mainly due to the potential loss of customers. In the case of Malaysia, for example, it has experienced significant financial losses due to cybercrime frauds, amounting to RM2.23 billion between 2017 and mid-2021, as reported by the Royal Malaysian Police. Furthermore, in the first quarter of 2022, Malaysia faced 8 million virus attacks and detected 57.2 botnets, of which small and medium-sized enterprises (SMEs) have been particularly vulnerable, with 84% experiencing cyber threat incidents (Strategic Institute for Asia Pacific, 2022). Other incidents have been reported involving the use of unauthorized programs to access servers or databases through certain mobile applications. Hackers frequently target activities such as downloading resources or programs from an unverified origin and developing unapproved software (Chai & Zolkipli, 2021; Ching & Zolkipli, 2021).

[1] Department of Communication and Media, Faculty of Languages and Communication, Universiti Pendidikan Sultan Idris (UPSI) Tanjong Malim, Perak, Malaysia. INTI International College Penang, 1-Z, Lebuh Bukit Jambul, Bukit Jambul, 11900 Bayan Lepas, Pulau Pinang.
[2] Department of Communication and Media, Faculty of Languages and Communication, Universiti Pendidikan Sultan Idris (UPSI) Tanjong Malim, Perak, Malaysia; E-mail: sitinoramalina@fbk.upsi.edu.my (Corresponding author)
[3] Department of Communication and Media, Faculty of Languages and Communication, Universiti Pendidikan Sultan Idris (UPSI) Tanjong Malim, Perak, Malaysia.

Journal of Ecohumanism
2024
Volume: 3, No: 3, pp. 1626– 1638
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i3.3327

Businesses, particularly SMEs, have modified their marketing strategies to utilize digital platforms such as websites, social media, banner ads, etc., not only to provide product or service information and maintain customer relationships (Filiz Bozkurt Bekoglu & Cemre Onaylı, 2016), as well as to reduce marketing expenses and coordination cost (Meyer et al., 2023). Despite these advantages, enterprises face a number of obstacles while utilizing digital business, including the possibility of cyberattacks, spammers, and illicit businesses (Fernandez De Arroyabe & Fernandez de Arroyabe, 2023; Kaur et al., 2023; Wilson et al., 2023). Moreover, with this transformation and global opportunity offered through digital business, small and medium-sized businesses are always becoming great targets for hackers (Fernandez De Arroyabe & Fernandez de Arroyabe, 2023; Tam et al., 2021; Wallang et al., 2022) because they lack cybersecurity-related measures to survive significant security incidents. The continuous use of information technology systems by SMEs has the potential to deliver substantial benefits but also exposes them to internet security risks. This problem is most prominent in emerging nations, especially among small and medium-sized businesses (SMEs), which frequently lack the funds to purchase and deploy cybersecurity equipment (Westerlund & Rajala, 2014). Moreover, many individuals assume they do not know how to defend their Internet system or are uninformed of the repercussions of not utilizing Internet security software (Bada et al., 2019). Thus, the present study seeks to:

a) To identify the level of knowledge, perceived usefulness, and perceived ease of use towards cybersecurity among SME Entrepreneurs in Perak.
b) To investigate the relationship between knowledge and perceived usefulness towards digital business and cybersecurity among SME Entrepreneurs in Perak.
c) To examine the relationship between knowledge and perceived ease of use towards digital business and cybersecurity among SME Entrepreneurs in Perak.
d) To find out the relationship between knowledge and adoption of cybersecurity among SME Entrepreneurs in Perak.

Following the present research objectives, the authors have hypothesized:

H1: The knowledge is positively correlated with the perceived usefulness of digital business among SMEs

H2: The knowledge is positively correlated with the perceived usefulness of cybersecurity among SMEs

H3: The knowledge is positively associated with the perceived ease of use of digital business among SMEs

H4: The knowledge is positively associated with the perceived ease of use of cybersecurity among SMEs

H5: There is a positive relationship between knowledge and the adoption of cybersecurity among SMEs

Literature Review

Digital Business and Marketing

Digital platforms serve as the nexus for connecting various entities, typically suppliers and consumers, to facilitate commercial interactions. In the present business landscape, leveraging digital expertise, technologies, and tools is essential for enterprise leaders and pioneers. It allows them to transform their businesses, leading to improved experiences for customers, employees, and ecosystem partners, while also driving cost efficiencies (Mishra & Tripathi, 2020). For example, around a quarter-century ago, the concept of purchasing books online through Amazon was a novel and relatively untested idea. Back then, it would have been difficult to envision that Amazon would eventually emerge as one of the most valuable and influential companies on a global scale (Verhoef & Bijmolt, 2019). However, Amazon's remarkable ascent is not an isolated case. Indeed, as highlighted by the 2018 Interbrand equity rankings, the top-tier positions are dominated by digital giants like Apple, Google, and Amazon—relatively three companies were all digital and reasonably new in comparison to long-established firms like Coca-Cola, General Motors, and Exxon Mobil (Verhoef & Bijmolt, 2019). This transformation highlights the significant impact of digital firms on the global business landscape.

In the era of digital business, the power of digitalization becomes evident as it unlocks new avenues for firms. These opportunities allow them to engage with international business and streamline capital investments essential for effective competition in overseas markets. For instance, through virtual avenues like firm-specific websites or platform complementors, digital business strategies can magnify export potentials, thereby significantly broadening the horizon of potential customers a firm can cater to (Meyer et al., 2023). Furthermore, in the context of digital business, e-commerce stands in stark contrast to traditional retail. Unlike the conventional methods, the majority of e-commerce interactions, from the pre-purchase information search to the actual purchase and even post-purchase stages like feedback and after-

Journal of Ecohumanism
2024
Volume: 3, No: 3, pp. 1626– 1638
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i3.3327

sales services, are managed virtually (Ayob, 2021). Furthermore, through digital business, the strategic use of social proof by marketers plays a crucial role. It serves not only to address consumers' apprehensions but also to establish trust in the products and services being offered (Dwivedi et al., 2021). For instance, in the e-commerce sector, social proof is harnessed as a persuasive technique. This is achieved by prominently showcasing testimonials and product reviews, thereby nudging potential customers toward making informed purchase decisions based on the experiences of others (Malodia et al., 2022). As such, digital marketing encompasses a wide array of activities that leverage electronic devices and online resources which is further explained in the next paragraph.

Digital marketing is the cornerstone of modern digital business strategies. It involves promoting products and services through digital channels, primarily the Internet, but also mobile devices, display advertising, and various other digital platforms. In today's dynamic business environment, the digital marketing landscape is in a perpetual state of transformation, driven by the rapid pace of technological advancements. As technology evolves, it brings about significant shifts in the way companies engage with their audiences and promote their products and services. Businesses engage with their current and potential customers through online platforms like search engines, social media, email, and various websites (Terrance et al., 2018). This practice is essential for reaching and engaging with customers who spend a significant amount of their time online. Digital marketing takes various forms, including content marketing, email marketing, online advertising, landing page marketing, smartphone marketing, affiliate marketing, and viral marketing (Dwivedi et al., 2021). Additionally, it encompasses crucial elements like search engine optimization (SEO), search engine marketing (SEM), and social media marketing (SMM) (Terrance et al., 2018). By employing a diverse range of techniques such as banners, articles, videos, images, flash animation, and more, online marketing becomes a powerful means of attracting potential clients to a digital business (Terrance et al., 2018), facilitating effective communication and engagement with the online audience (Dunakhe & Panse, 2022).

It is essential to note that, regardless of how sophisticated the digital technology becomes, the primary importance lies in ensuring that users remain safe and secure while navigating the digital space. Making wise choices is crucial to maximizing the use of technology while minimizing cyber risks (Maliki et al., 2023). Five key facets of this transformation stand out: the escalating need for information, the proliferation of information sources, heightened concerns about data security, the ubiquitous use of mobile devices, and the expanding role of social media in industrial purchasing (Dunakhe & Panse, 2022). These changes underscore the critical role of cyber security and innovation in navigating the ever-shifting terrain of digital marketing which is further explained in the next sub-section.

Cybersecurity among Small and medium-sized enterprises (SMEs)

Looking at the perspective of digital business, the term 'cybersecurity' represents a comprehensive approach to security practices that encompasses both offensive and defensive actions in the context of information technology and operational technology environments and systems (Schatz et al., 2017). This definition positions cybersecurity as a broader framework that goes beyond individual security disciplines like information security and IT security. Instead, it provides a holistic perspective on safeguarding digital assets, data, and operations, which is particularly crucial in the increasingly interconnected and technologically driven landscape of modern business fields (Schatz et al., 2017). Understanding cybersecurity in this context is vital for digital enterprises seeking to protect their digital infrastructure, customer data, and intellectual property from evolving threats in the digital age.

Today, small and medium-sized enterprises (SMEs) are reported as the new big target for cyberattacks, being among the most vulnerable in terms of their cybersecurity risk (Fernandez De Arroyabe & Fernandez de Arroyabe, 2023; Tam et al., 2021; Wallang et al., 2022). They often become primary targets of various attacks due to their limited resources and, more importantly, their limited ability to manage complex technical issues (Candra et al., 2023). Even worse, the existence of the dark web, which provides anonymity and acts as a gateway to the criminal world, exacerbates the challenges faced by SMEs (Rajamanickam & Zolkipli, 2021). In the face of cybercriminals employing various 'old school' tactics, the battleground of today's cyberwars extends beyond the technicalities of breaching routers, switches, servers, or websites. It involves a more subtle and cunning approach, where perpetrators exploit human interaction, capitalizing on their social skills to extract sensitive information from their targets (Alsobeh et al., 2023). This technique, known as social engineering, hinges on hackers' ability to seamlessly blend into various roles within an organization, whether it's posing as a new employee, a reformer, a scholar, or even a seemingly legitimate

Journal of Ecohumanism
2024
Volume: 3, No: 3, pp. 1626– 1638
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i3.3327

representative of the company, complete with credentials (Alsobeh et al., 2023). These social engineering attacks come in various forms, from widely recognized phishing attempts to tactics that exploit human greed, curiosity, or even the act of rummaging through discarded materials (dumpster diving). It's a world where deception and manipulation are the primary weapons, and it poses a significant challenge to digital businesses striving to protect their assets and information in an interconnected and vulnerable landscape (Alsobeh et al., 2023). Understanding and countering these social engineering techniques have become paramount in the ongoing battle to safeguard the integrity and security of digital enterprises.

As SMEs navigate the path of digital transformation, leveraging its numerous benefits such as enhanced management efficiency, better service and product delivery to customers, and fostering an innovative culture, they simultaneously grapple with significant challenges (Ta & Lin, 2023). These challenges range from capital constraints, scarcity of highly skilled professionals, and a deficit in information communication technology expertise (Ta & Lin, 2023). Thus, the relationship between cybersecurity and small and medium-sized enterprises (SMEs) is a contentious issue, as highlighted by various studies (Adleena Huzaizi et al., 2021; Fernandez De Arroyabe & Fernandez de Arroyabe, 2023; Henson & Garfield, 2016; Shojaifar, 2020; Wallang et al., 2022). Many SMEs do not prioritize information security, resulting in minimal cybersecurity budgets (Fernandez De Arroyabe & Fernandez de Arroyabe, 2023; Shojaifar, 2020; Wilson et al., 2023) This lack of concern is often rooted in the belief that the level of risk is relatively low compared to larger companies, leading to a false sense of security (Fernandez De Arroyabe & Fernandez de Arroyabe, 2023; Wilson et al., 2023). Additionally, SMEs frequently struggle with implementing cybersecurity processes due to the diversity and quantity of devices in their networks, as well as a tendency to deviate from established procedures and standards (Fernandez De Arroyabe & Fernandez de Arroyabe, 2023; Tam et al., 2021). Consequently, SMEs face challenges in adhering to cybersecurity best practices and standards.

In the case of Malaysia, the swift advancement of digitalization has necessitated businesses, including SMEs, to adapt significantly and quickly to technological shifts. These adaptations encompass the adoption of cloud solutions, enhancements in network connectivity, and website overhauls (Wallang et al., 2022). In the year 2022, Malaysia's SMEs achieved a remarkable growth rate of 11.6% (Bernama, 2023). What makes this achievement even more noteworthy is that it outpaced the overall Gross Domestic Product (GDP) growth rate of the entire country, which stood at 8.7% (Mohamad Hafizi, 2023). This substantial growth underscores the increasingly pivotal role that SMEs are playing in propelling economic development within Malaysia. Furthermore, the contribution of SMEs to the nation's GDP saw a significant uptick, climbing from 37.41% in 2021 to 38.4% in 2022 (Bernama, 2023). In terms of value-added, SMEs contributed a substantial RM580.4 billion to the economy in 2022, a notable increase compared to the RM520 billion recorded in the previous year (Bernama, 2023). Yet, these transformations have also heightened the risk of cyberattacks, endangering the security of numerous enterprises. Previously, the World Economic Forum's Global Risk Reports 2021 posits that cybersecurity failures might soon become the world's fourth most pressing threat (Wallang et al., 2022).

In the rapidly digitizing business environment, cybersecurity becomes paramount. As SMEs undergo digital transformation, their digital footprints expand, leading to potential vulnerabilities. Given the constraints SMEs face, such as limited resources (Waqas et al., 2022), they often become prime targets for cybercriminals. Ensuring robust cybersecurity measures is not merely about safeguarding business operations but is also crucial for preserving customer trust, protecting sensitive data, and ensuring regulatory compliance (Ta & Lin, 2023). Therefore, as SMEs identify the risk of cyberattacks in their digital transformation journey, integrating cybersecurity measures should be at the forefront. The digital opportunities that transformation offers can only be fully realized when underpinned by strong security protocols (Ta & Lin, 2023). Cybersecurity measures help protect SMEs from the growing threats of cyberattacks, ensuring the continuity of their operations and maintaining the trust of their customers and partners. In this context, cybersecurity becomes not just a technological necessity but a strategic imperative for SMEs navigating the digital landscape.

Technology Acceptance Model (TAM)

The entire research process was guided by a theoretical framework, which serves as a navigational tool. Within this framework, concepts and their respective definitions form the foundation elements.

Journal of Ecohumanism
2024
Volume: 3, No: 3, pp. 1626– 1638
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i3.3327

Additionally, the incorporation of pertinent prior research from the relevant academic field enriches the framework's components (Creswell & Creswell, 2018). This theoretical framework demonstrates a deep comprehension of ideas and concepts relevant to the research question, as well as their connections to broader knowledge domains under investigation. The Technology Acceptance Model (TAM) serves as the foundational framework for understanding the influence of external factors on technology adoption decisions. Its core principles are firmly grounded in economic, utilitarian, and attitudinal factors (Awa et al., 2015). Specifically, an individual's inclination to use a particular application is determined and predicted by their perception of the technology's usefulness and its ease of use (Alnemer, 2022; Awa et al., 2015; Cho et al., 2022; Davis, 1985; Ritz et al., 2019; Thathsarani & Jianguo, 2022). Additionally, SMEs often struggle to adapt to the swift technological advancements, presenting challenges in catering to innovative requirements, which in turn impacts their long-term sustainability (Waqas et al., 2022).

This theory highlights the integration of information technologies and associated tools, like the incorporation of microcomputers and the Internet. The TAM is based on the theoretical foundations of Fishbein and Ajzen's (1975) theory of reasoned action, which explores connections between various components like belief, attitude, intention, and behavior (as shown in Figure 1). Davis (1985) notably highlighted the interplay between usefulness, ease of use, attitude, and the intention to use technology as influential beliefs in shaping technology adoption. Initially, TAM was employed within specific occupational categories, such as office workers or professionals in computer-related roles, but over time, it has found widespread application in various domains (Cho et al., 2022). Another study highlighted the TAM, as a framework that elucidates how users of information systems assess and utilize technology, with the key factors for embracing or declining a specific technology being their 'perceived usefulness' and 'perceived ease of use' (Davis, 1987; Davis et al., 1989; Thathsarani & Jianguo, 2022) Perceived usefulness (PU) refers to the extent to which an individual thinks that employing a system could boost their efficiency and contribute positively to an organization, given the system is used appropriately. This illustrates how integrating technology into businesses can boost user efficiency, elevate performance, and amplify advantages. Meanwhile, the second dimension of TAM, Perceived ease of use (PEOU), describes the extent to which an individual feels that using a particular technology doesn't require significant physical or mental exertion (Davis, 1985; Nazir & Khan, 2022).

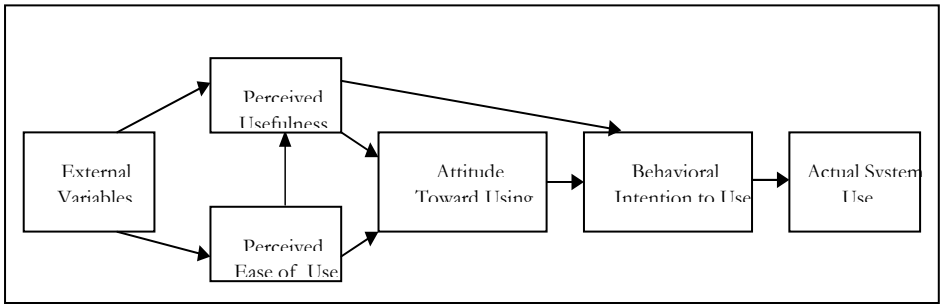

Fig. 1. Original technology acceptance model (TAM)

Fundamentally, the concept within TAM is that the easier the technology is, the more advantageous it becomes for the user (Ritz et al., 2019). With the removal of technical obstacles, a crucial aspect of leveraging this increasing capability lies in our capacity to develop applications that individuals are inclined to employ. As technical obstacles diminish, the key to tapping into this growing capability is our capacity to develop applications that users are eager to adopt (Davis et al., 1989). Determining the right functional and interface qualities for end-user systems has turned out to be more intricate and nuanced than initially anticipated (Davis et al., 1989). The challenge of adopting digital business is not so much about using technology but rather knowing which platforms to choose and how to optimize their use (Davis et al., 1989; Ritz et al., 2019). Small business owners and operators can first familiarize themselves with digital business by engaging in personal social media accounts, and then transition to accounts dedicated to their business. In this setting, actual technology use implies that the small business leader is engaging in digital business while implementing cyber security measures to safeguard it (Ritz et al., 2019). In light of the challenges

Journal of Ecohumanism
2024
Volume: 3, No: 3, pp. 1626– 1638
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i3.3327

encountered during the lockdown phase, the evolution of new technology adoption has become crucial for individuals, businesses, governments, and economies through digital means (Thathsarani & Jianguo, 2022). Leveraging digital technology is certainly provide SMEs with essential insights, knowledge, enhanced relationships with suppliers and customers, better collaboration, and boosted productivity and efficiency.

In the context of small and medium-sized enterprises (SMEs), the Internet plays a pivotal role in helping them devise digital business strategies. The potential advantages of digital business for SMEs are manifold. These benefits encompass cost reductions, especially in procurement, communication, inventory management, and search activities (Awa et al., 2015; Dwivedi et al., 2021; Kraft et al., 2022). Additionally, digital business can lead to improved product quality and customer service, provide value-added information, and stimulate innovation through network externalities and knowledge sharing (Awa et al., 2015). Employing the TAM framework can shed light on how these external variables impact the adoption of technology in the realm of digital business and its resulting benefits for SMEs.

Methodology

Quantitative Research design

Quantitative research involves gathering and analyzing numerical data to describe, explain, predict, or control variables and phenomena of interest (Creswell & Creswell, 2018). Researchers conducting quantitative studies aim to describe current situations, establish relationships between variables, and sometimes elucidate causal connections. This research type is primarily concerned with providing detailed descriptions and explanations about the phenomenon under investigation, often with a strong degree of certainty (Salkind, 2013). Survey research primarily aims to depict the attributes of a collective or population. This research method is predominantly quantitative, involving the distribution of surveys or questionnaires by the researcher to a sample, or occasionally the entire population, to outline their attitudes, views, actions, encounters, or other qualities of the group (Creswell & Creswell, 2018).

In this study, a quantitative approach was chosen and employed during the formulation of the questionnaire, which acted as the primary tool for data collection. Before embarking on the questionnaire design, the research objectives and research questions serve as our guidelines in preparing the entire questionnaire. More importantly, the questionnaire questions were aligned with the study variables, where each question sought to capture a specific aspect of the construct (Allen, 2017). Formulating quantitative survey questionnaires is a meticulous process that involves a deep understanding of research objectives, variable definitions, and an informed selection of question types, wording, and response scales. A well-constructed questionnaire is the foundation of sound research, ensuring the data collected is meaningful and actionable which is further explained in the next sub-section. The initial stage of creating the research questionnaire focused on crafting items that resonated with the undertaken study. The aim was to collect data and assess the participants' knowledge, perceived usefulness, and perceived ease of use towards cybersecurity among SME Entrepreneurs in Perak. The questionnaire was constructed based on six(6) sections allocated into sections A, B, C, D, E and F as demonstrated in Table 1. This questionnaire has been adopted from several past studies (Filiz Bozkurt Bekoglu & Cemre Onaylı, 2016; Pham et al., 2021; Zwilling et al., 2020) and revised according to the Malaysian context.

Table 1. Division of questionnaire based on the construct

No	Section	Construct
1	A	Demographic characteristics
2	B	Knowledge of Cyber Security
3	C	Cyber Security (Perceived usefulness)
4	D	Digital Business (Perceived usefulness)
5	E	Cyber Security (Perceived ease of use)
6	F	Digital Business (Perceived ease of use)

Journal of Ecohumanism
2024
Volume: 3, No: 3, pp. 1626– 1638
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i3.3327

Sampling and Data collection

The survey questionnaires were handed out to 500 participants, and the survey yielded a response rate of 400 individuals (after filtering out completed questionnaires). All of these participants are small and medium-sized enterprise (SME) entrepreneurs located in Perak, Malaysia. The estimated completion time for the questionnaire ranged between 15 to 25 minutes. The study population consists of small and medium-sized enterprise entrepreneurs in Perak state 75,140 have been registered as entrepreneurs. Therefore, this study was conducted by using Krejcie & Morgan, 1970 for the population size, which is 400 respondents. For this investigation, we adopted a mixed sampling design by combining both probability random sampling and non-probability sampling procedures for the selection of a sample. First, the participants were randomly selected from the database of SME business owners located in the state of Perak using systematic random sampling. After that, selected participants from the database were again selected based on certain criteria: they must be registered as small and medium businesses (SMEs), they must use digital marketing for their companies, they must have at least two social media platforms, and their companies must have been in operation for more than six months.

Table 2. The number of SME Establishments by State

State	Total SMEs	%	State	Total SMEs	%
Selangor	179,271	19.8	Negeri Sembilan	32,721	3.6
WP Kuala Lumpur	133,703	14.7	Melaka	31,361	3.5
Johor	98,190	10.8	Terengganu	29,324	3.2
Perak	75,140	8.3	Perlis	6,808	0.8
Pulau Pinang	66,921	7.4	WP Labuan	2,567	0.3
Sarawak	61,036	6.7	WP Putrajaya	1,236	0.1
Sabah	55,702	6.2	**Total SMEs**	**907,065**	**100.0**
Kedah	48,894	5.4			
Kelantan	46,618	5.1			
Pahang	37,573	4.1			

Source: Economic Census 2016: Profile of Small and Medium Enterprises (reference year 2015), Department of Statistics, Malaysia

The reason for opting to study the state of Perak as the research location is underpinned by the previous report's findings. In 2020, Perak was reported to be among the top 5 states with the highest number of cybercrime incidents (The Star, 2023). These incidents included various cyberattacks and offenses against individuals, with a noticeable upward trend. While experts suggest that the COVID-19 pandemic might have contributed to this surge, they also acknowledge the influence of other factors. Furthermore, in the past five years, several significant data security breaches have occurred in well-known companies. Additionally, Perak stands out in Malaysia for its substantial concentration of small and medium-sized businesses (SME Corporation Malaysia, 2019; The Star, 2023)

Data analysis

Data analysis is the systematic process of organizing, merging, selecting, and arranging collected data. In the course of this study, we employed Statistical Package for the Social Sciences (SPSS) version 29 for the analysis of questionnaire responses. Researchers are drawn to SPSS for its robust statistical analysis and data processing capabilities. For this investigation, we employed two data types: descriptive statistical analysis and correlation analysis. Descriptive statistics were utilized to examine respondents' backgrounds and their level of knowledge of cyber security. This analysis included parameters such as total scores, percentages, and frequencies, providing an overview of the data. As a result, correlation analysis has been utilized in order to investigate the nature of the link.

Journal of Ecohumanism
2024
Volume: 3, No: 3, pp. 1626– 1638
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i3.3327

Results and Discussion

Result/findings

The respondents consist of 400 entrepreneurs from Perak. These demographic factors are broken down into categories such as gender, age, and the number of years in business.

Table 3. Frequency distribution of gender among participants

Gender	Frequency	Percent
Male	171	42.8
Female	229	57.3
Total	**400**	**100.0**

Table 3 displays the distribution of respondent populations by gender. The data reveals that out of a total of 400 respondents, 171 (42.8% of the respondents) were males, and 229 (57.3% of the respondents) were females. This indicates that a significant majority of respondents are female, while the male respondents constitute a relatively smaller portion.

Table 4. Frequency distribution of age

Age	Frequency	Percent
18-25	126	31.5
26-35	160	40.0
36-45	55	13.8
46-55	46	11.5
55 and above	13	3.3
Total	**400**	**100.0**

The age distribution of the respondents is presented in Table 4. It is notable that all the respondents fall within the age range of 26 to 35, representing the largest group, with 160 respondents (40.0%). On the other hand, the age category of entrepreneurs aged 55 and above constitutes the smallest segment, with only 13 respondents (3.3% of the total respondents) providing their input.

Table 5. Frequency distribution of years of business operation

Business operation (years)	Frequency	Percent
Under 5	243	60.8
5-10	97	24.3
11-15	17	4.3
16-20	22	5.5
21 and above	21	5.3
Total	**400**	**100.0**

Table 5 provides a breakdown of the number of years respondents have spent in their businesses. When considering the duration of their business operations, the findings reveal that a significant majority of respondents (243, equivalent to 60.8% of the total) have been in business for less than five years. Conversely, the sample included 21 respondents (5.3%) who possessed over 21 years of experience in various business operations.

Table 6. Descriptive statistics of knowledge, perceived usefulness, Perceived ease of use and Adoption of cybersecurity

Variables	N	Mean	Std. Deviation
Knowledge	400	91.01	11.44
Perceived usefulness	400	87.36	11.04
Perceived ease of use	400	77.02	19.65
Adoption of cybersecurity	400	46.27	6.40
Valid N (list wise)	**400**		

Journal of Ecohumanism
2024
Volume: 3, No: 3, pp. 1626– 1638
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i3.3327

The descriptive statistics for knowledge, perceived usefulness, perceived ease of use, and adoption of cybersecurity are presented in Table 6. The descriptive statistics suggest that the overall mean score for knowledge is 91.02, and the standard deviation is 11.45. The provided descriptive statistics reveal that the mean score for perceived usefulness is 87.36, with a standard deviation of 11.05. For perceived ease of use, the average score is 77.02, accompanied by a standard deviation of 19.66. As for the mean score of the adoption of cybersecurity measures, it stands at 6.40, with a standard deviation of 6.40. In general, knowledge garnered a higher mean score compared to perceived usefulness, perceived ease of use, and the adoption of cybersecurity measures. Notably, the score for the adoption of cybersecurity exhibited the least variability, as indicated by the standard deviation.

Table 7. Correlations between Knowledge and Perceived Usefulness of Digital Business and Cybersecurity

Variables		Knowledge	Perceived usefulness digital business	Perceived usefulness cyber security
Knowledge	Pearson Correlation Sig. (2-tailed)	1	.488** .000	.644 .000
Perceived usefulness Digital business	Pearson Correlation Sig. (2-tailed)	.488** .000	1	
Perceived usefulness Cyber security	Pearson Correlation Sig. (2-tailed)	.644 .000		1
N		**400**	**400**	**400**

** Correlation is significant at the 0.01 level (2-tailed).

The relationships between knowledge and the perceived usefulness of digital marketing are outlined in Table 7. The findings of the test using Pearson's correlation coefficient indicate that there is a significant positive linear relationship between knowledge and the perceived usefulness of digital business (r .488), $p<0.01$. There is a moderate positive relationship between knowledge and the perceived usefulness of digital business. Furthermore, the relationships between knowledge and the perceived usefulness of cybersecurity show that there is a significant positive linear relationship between knowledge and the perceived usefulness of cybersecurity (r .664), $p<0.01$. Knowledge and perceived usefulness of cyber security are strong positive relationships to one another in a favorable way.

Table 8. Correlations between Knowledge and Perceived Ease of Use of Digital Business and Cybersecurity

Variables		Knowledge	Perceived Ease of Use (digital business)	Perceived Ease of Use (cyber security)
Knowledge	Pearson Correlation Sig. (2-tailed)	1	.348** .000	.465 .000
Perceived Ease of Use Digital business	Pearson Correlation Sig. (2-tailed)	.348** .000	1	
Perceived Ease of Use Cyber security	Pearson Correlation Sig. (2-tailed)	.465 .000		1
N		**400**	**400**	**400**

** Correlation is significant at the 0.01 level (2-tailed).

Table 8 reports the correlations between knowledge and perceived ease of use of digital marketing. The results of the Pearson's correlation coefficient test show there is a significant positive linear relationship between knowledge and perceived ease of use of cybersecurity. (r .348), $p<0.01$. There is a moderate

Journal of Ecohumanism
2024
Volume: 3, No: 3, pp. 1626– 1638
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i3.3327

positive relationship between knowledge and perceived ease of use of digital marketing. Moreover, Table 8 also reports the correlations between knowledge and perceived ease of use of cybersecurity. The finding shows that there is a significant positive linear relationship between knowledge and perceived ease of use of cybersecurity. (r .465), p<0.01. There is a moderate positive relationship between knowledge and perceived ease of use of cybersecurity.

Table 9. Correlations between knowledge and adoption of cybersecurity

Variables		Knowledge	Adoption of cybersecurity
Knowledge	Pearson Correlation Sig. (2-tailed)	1	.031 .535
Adoption of cybersecurity	Pearson Correlation Sig. (2-tailed)	.031 .535	1
N		**400**	**400**

Table 9 reports the correlations between knowledge and adoption of cybersecurity. The results of Pearson's correlation show there is no significance, however, there is a positive linear relationship between knowledge and adoption of cybersecurity. (r .348), p<0.01. However, there is a weak positive relationship between knowledge and the adoption of cybersecurity.

Table 10. Hypotheses based on the present findings

Hypotheses	Coefficient	Accepted ?
H1: The knowledge is positively correlated with the perceived usefulness of digital business among SMEs	.488	Yes
H2: The knowledge is positively correlated with the perceived usefulness of cybersecurity among SMEs	.644	Yes
H3: The knowledge is positively associated with the perceived ease of use of digital business among SMEs	.348	Yes
	.465	Yes
H4: The knowledge is positively associated with the perceived ease of use of cybersecurity among SMEs	.031	Yes
H5: There is a positive relationship between knowledge and the adoption of cybersecurity among SMEs		
N	**400**	**400**

In summary, Table 10 provides the five (5) hypotheses that have been supported by the research findings, demonstrating positive relationships and associations between knowledge and various aspects of digital business and cybersecurity adoption among SMEs.

Conclusion and Suggestions for Future Research

The scope of online activities is continuously expanding, underscoring the increasing importance of equipping business owners with knowledge, perceived ease of use, perceived usefulness, and the adoption of cybersecurity measures to mitigate the risks associated with cybercrimes. In response, collaborative efforts are crucial to address this issue comprehensively, especially when it comes to disseminating extensive knowledge to customers, particularly within the realm of digital small and medium enterprises. These SME entrepreneurs are particularly susceptible to cybercrime risks, given their engagement in online sales, financial transactions, and constant interaction with evolving social media platforms (Adleena Huzaizi et

Journal of Ecohumanism
2024
Volume: 3, No: 3, pp. 1626– 1638
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v3i3.3327

al., 2021; Fernandez De Arroyabe & Fernandez de Arroyabe, 2023; Henson & Garfield, 2016; Shojaifar, 2020; Wilson et al., 2023). Therefore, a shared responsibility exists among all relevant stakeholders to enhance the level of knowledge among customers and individuals responsible for ensuring the safety of the Internet by developing more secure policies and procedures.

From the findings, it becomes evident that a significant proportion of respondents exhibit a commendable level of knowledge concerning both cybersecurity and digital marketing in a broader context. This pattern is consistent across the board. Consequently, it is imperative for entrepreneurs to be acutely mindful of issues pertaining to the privacy and security of customer's personal information, as well as other sensitive aspects accessible through social media applications. It is highly probable that a substantial majority of entrepreneurs possess a certain degree of knowledge regarding digital marketing and cybersecurity. However, the presence of digital monitoring or social surveillance poses potential risks to the security and confidentiality of their routine business operations, particularly when sharing information on various social media platforms, even though only a minority remains oblivious to its existence. In summary, the findings of this study were in alignment with the expected outcomes (Adleena Huzaizi et al., 2021; Fernandez De Arroyabe & Fernandez de Arroyabe, 2023; Henson & Garfield, 2016; Shojaifar, 2020; Wilson et al., 2023). Previous research predominantly focused on marketing from the customer's perspective, exploring aspects such as how retailers promote their diverse products and services. Nevertheless, delving into the security concerns arising from digital marketing represents a vital supplementary step, precisely what the current researchers have undertaken. Furthermore, the surge in the adoption of digital payment methods heightens the susceptibility to cybercrimes, particularly since many new users fail to implement the requisite security measures for their financial transactions. Hence, this study concentrated on both domains, encompassing digital marketing and cybersecurity.

The scope of this study could be broadened by examining entrepreneurs in diverse locales, contrasting between rural and urban settings, to gauge the depth of cybersecurity expertise prevalent in these regions. A notable limitation encountered in the study was confined to the state of Perak; future studies should endeavor to broaden its scope, encompassing a larger dataset from across Malaysia. Researchers can also delve deeper into the factors shaping awareness, knowledge, attitudes, and behaviors concerning cybersecurity, especially in the realm of social media network usage. Further inquiries are recommended to unearth the relationship between sociodemographic attributes and the cybersecurity practices of both entrepreneurs and their clientele. Wherever an institution is designated as a research base, scholars might consider integrating varied research techniques like interviews or observational approaches. For entrepreneurs, knowledge, attitude, practices, and training are deemed essential for disseminating pertinent information to their audience, especially in endeavors to elevate cyberspace risk awareness. When advertising campaigns convey relevant insights, they enhance users' awareness and comprehension of the topic. This, in turn, could bolster the overall safety of online users.

Acknowledgment

This research project was conducted under the support of the Fundamental Research Grants Scheme (FRGS/1/2020/SS0/UPSI/02/5) granted by the Ministry of Education of Malaysia to facilitate the completion of a postgraduate study. The authors express their appreciation to Universiti Pendidikan Sultan Idris (UPSI) for their assistance in administering the grant and facilitating the successful completion of this project.

References

Adleena Huzaizi, A. H., Ahmad Tajuddin, S. N. A., Bahari, K. A., Manan, K. A., & Abd Mubin, N. N. (2021). Cyber-Security Culture towards Digital Marketing Communications among Small and Medium-Sized (SME) Entrepreneurs. Asian Culture and History, 13(2), 20. https://doi.org/10.5539/ach.v13n2p20

Allen, M. (2017). The SAGE Encyclopedia of Communication Research Methods. SAGE Publications Ltd.

Alnemer, H. A. (2022). Determinants of digital banking adoption in the Kingdom of Saudi Arabia: A technology acceptance model approach. Digital Business, 2(2). https://doi.org/10.1016/j.digbus.2022.100037

Alsobeh, A. M. R., Alazzam, I., Shatnawi, A. M. J., & Khasawneh, I. (2023). Cybersecurity awareness factors among adolescents in Jordan: Mediation effect of cyber scale and personal factors. Online Journal of Communication and Media Technologies, 13(2). https://doi.org/10.30935/ojcmt/12942

Awa, H. O., Ojiabo, O. U., & Emecheta, B. C. (2015). Integrating TAM, TPB and TOE frameworks and expanding their characteristic constructs for e-commerce adoption by SMEs. Journal of Science and Technology Policy Management, 6(1), 76–94. https://doi.org/10.1108/JSTPM-04-2014-0012

Ayob, A. H. (2021). E-commerce adoption in ASEAN: who and where? Future Business Journal, 7(1), 1–11. https://doi.org/10.1186/s43093-020-00051-8

Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). Cyber Security Awareness Campaigns: Why do they fail to change behaviour? 1–11. http://arxiv.org/abs/1901.02672

Bernama. (2023, July 27). KDNK PMKS Malaysia melonjak11.6 peratus kepada RM580.4 bilion pada 2022. Bernama.

Candra, Y. T. A., Wulandari, I., & Wafa, Z. (2023). Analysis of MSME Strategies in Responding to Crisis: A Case Study of MSME in Gunungkidul Regency. International Business Education …, 16(1), 12–21. https://ojs.upsi.edu.my/index.php/IBEJ/article/view/7664%0Ahttps://ojs.upsi.edu.my/index.php/IBEJ/article/download/7664/4423

Chai, K. Y., & Zolkipli, M. F. (2021). Review on Confidentiality, Integrity and Availability in Information Security. Journal of ICT In Education, 8(2), 34–42. https://doi.org/10.37134/jictie.vol8.2.4.2021

Ching, G. H., & Zolkipli, M. F. (2021). Review on Cryptography Techniques in Network Security. Journal of ICT in Education, 8(2), 125–135.

Cho, J., Cheon, Y., Jun, J. W., & Lee, S. (2022). Digital advertising policy acceptance by out-of-home advertising firms: a combination of TAM and TOE framework. International Journal of Advertising, 41(3), 500–518. https://doi.org/10.1080/02650487.2021.1888562

Creswell, J. W., & Creswell, J. D. (2018). Research Design Qualitative, Quantitative, and Mixed Methods Approaches. In SAGE Publications.

Davis, F. D. (1985). A technology acceptance model for empirically testing new end-user information systems: Theory and results. In Doctoral dissertation, Massachusetts Institute of Technology. https://doi.org/10.1126/science.146.3652.1648

Davis, F. D. (1987). User Acceptance of Information Systems: The Technology Acceptance Model (TAM). In University of Michigan. https://doi.org/10.1002/9781119678816.iehc0776

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User Acceptance of Computer Technology: A Comparison of Two Theoretical Models. Management Science, 35(8), 982–1003. https://doi.org/10.1287/mnsc.35.8.982

Dunakhe, K., & Panse, C. (2022). Impact of digital marketing – a bibliometric review. International Journal of Innovation Science, 14(3–4), 506–518. https://doi.org/10.1108/IJIS-11-2020-0263

Dwivedi, Y. K., Ismagilova, E., Hughes, D. L., Carlson, J., Filieri, R., Jacobson, J., Jain, V., Karjaluoto, H., Kefi, H., Krishen, A. S., Kumar, V., Rahman, M. M., Raman, R., Rauschnabel, P. A., Rowley, J., Salo, J., Tran, G. A., & Wang, Y. (2021). Setting the future of digital and social media marketing research: Perspectives and research propositions. International Journal of Information Management, 59(May 2020), 102168. https://doi.org/10.1016/j.ijinfomgt.2020.102168

Fernandez De Arroyabe, I., & Fernandez de Arroyabe, J. C. (2023). The severity and effects of Cyber-breaches in SMEs: a machine learning approach. Enterprise Information Systems, 17(3), 1–27. https://doi.org/10.1080/17517575.2021.1942997

Filiz Bozkurt Bekoglu, & Cemre Onaylı. (2016). Strategic Approach in Social Media Marketing and a Study on Successful Facebook Cases. European Scientific Journal, ESJ, 12(7), 261–274. https://doi.org/https://doi.org/10.19044/esj.2016.v12n7p261

Henson, R., & Garfield, J. (2016). What Attitude Changes Are Needed to Cause SMEs to Take a Strategic Approach to Information Security? Athens Journal of Business & Economics, 2(3), 303–317. https://doi.org/10.30958/ajbe.2-3-5

Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. Information Fusion, 97(April). https://doi.org/10.1016/j.inffus.2023.101804

Kraft, C., Lindeque, J. P., & Peter, M. K. (2022). The digital transformation of Swiss small and medium-sized enterprises: insights from digital tool adoption. Journal of Strategy and Management, 15(3), 468–494. https://doi.org/10.1108/JSMA-02-2021-0063

Maliki, N. K., Bahari, K. A., Ali, R., Ahmad Tajuddin, S. N. A., Mohamed Hamoud Al-Majdhoub, F., & Balraj Baboo, S. (2023). Tahap Kewarganegaraan Digital dalam Kalangan Remaja 14 Tahun di Malaysia. EDUCATUM Journal of Social Sciences, 9(2), 94–105. https://doi.org/10.37134/ejoss.vol9.2.9.2023

Malodia, S., Kaur, P., Ractham, P., Sakashita, M., & Dhir, A. (2022). Why do people avoid and postpone the use of voice assistants for transactional purposes? A perspective from decision avoidance theory. Journal of Business Research, 146(April), 605–618. https://doi.org/10.1016/j.jbusres.2022.03.045

Meyer, K. E., Li, J., Brouthers, K. D., & Jean, R. J. "'Bryan.'" (2023). International business in the digital age: Global strategies in a world of national institutions. Journal of International Business Studies, 54(4), 577–598. https://doi.org/10.1057/s41267-023-00618-x

Mishra, S., & Tripathi, A. R. (2020). Literature review on business prototypes for digital platform. Journal of Innovation and Entrepreneurship, 9(1). https://doi.org/10.1186/s13731-020-00126-4

Mohamad Hafizi, M. S. (2023, July 27). KDNK PMKS melonjak 11.6 peratus. Utusan Malaysia. https://www.utusan.com.my/ekonomi/2023/07/kdnk-pmks-melonjak-11-6-peratus/

Nazir, M. A., & Khan, M. R. (2022). Identification of roles and factors influencing the adoption of ICTs in the SMEs of Pakistan by using an extended Technology Acceptance Model (TAM). Innovation and Development. https://doi.org/10.1080/2157930X.2022.2116785

Pham, H. C., Ulhaq, I., Nguyen, M. N., & Nkhoma, M. (2021). An Exploratory Study of the Effects of Knowledge Sharing Methods on Cyber Security Practice. Australasian Journal of Information Systems, 25(2017), 1–23. https://doi.org/10.3127/ajis.v25i0.2177

Rajamanickam, D. S., & Zolkipli, M. F. (2021). Review on Dark Web and Its Impact on Internet Governance. Journal of ICT In Education, 8(2), 13–23. https://doi.org/10.37134/jictie.vol8.2.2.2021

Ritz, W., Wolf, M., & McQuitty, S. (2019). Digital marketing adoption and success for small businesses: The application of the do-it-yourself and technology acceptance models. Journal of Research in Interactive Marketing, 13(2), 179–203. https://doi.org/10.1108/JRIM-04-2018-0062

Salkind, N. (2013). Quantitative Research Methods. Encyclopedia of Educational Psychology. https://doi.org/10.4135/9781412963848.n224

Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a More Representative Definition of Cyber Security. The Journal of Digital Forensics, Security and Law, 12(2), 52–74. https://doi.org/10.15394/jdfsl.2017.1476

Shojaifar, A. (2020, July 16). SMEs Confidentiality Issues and Adoption of Good Cybersecurity Practices. Computers and Society. https://arxiv.org/abs/2007.08201

SME Corporation Malaysia. (2019). SME Annual Report 2018/2019: Entrepreneurship Driving SMEs. Official Website SMEcorp Malaysia, 206.

Strategic Institute for Asia Pacific. (2022). Policy Brief on Cybersecurity and Digital Trust.

Ta, V. A., & Lin, C. Y. (2023). Exploring the Determinants of Digital Transformation Adoption for SMEs in an Emerging Economy. Sustainability (Switzerland), 15(9), 1–13. https://doi.org/10.3390/su15097093

Tam, T., Rao, A., & Hall, J. (2021). The good, the bad and the missing: A Narrative review of cyber-security implications for australian small businesses. In Computers and Security (Vol. 109, p. 102385). Elsevier Advanced Technology. https://doi.org/10.1016/j.cose.2021.102385

Terrance, A. R., Shrivastava, S., & Mishra, A. (2018). Importance of Search Engine Marketing in the Digital World. Proceedings of the First International Conference on Information Technology and Knowledge Management, 14, 155–158. https://doi.org/10.15439/2017km24

Thathsarani, U. S., & Jianguo, W. (2022). Do Digital Finance and the Technology Acceptance Model Strengthen Financial Inclusion and SME Performance? Information (Switzerland), 13(8). https://doi.org/10.3390/info13080390

The Star. (2023, May 25). SMEs in Perak seeing better business | The Star. The Star. https://www.thestar.com.my/metro/metro-news/2023/05/25/smes-in-perak-seeing-better-business

Verhoef, P. C., & Bijmolt, T. H. A. (2019). Marketing perspectives on digital business models: A framework and overview of the special issue. International Journal of Research in Marketing, 36(3), 341–349. https://doi.org/10.1016/j.ijresmar.2019.08.001

Wallang, M., Shariffuddin, M. D. K., & Mokhtar, M. (2022). Cyber security in Small and Medium Enterprises (SMEs): What's good or bad? Journal of Governance and Development (JGD), 18(1), 75–87. https://doi.org/10.32890/jgd2022.18.1.5

Waqas, A., Halim, H., & Ahmad, N. (2022). Design leadership and SMEs Sustainability; Role of Frugal Innovation and Technology Turbulence. International Journal of Systematic Innovation, 7(4), 1–17. https://doi.org/10.6977/IJoSI.202212_7(4).0001

Westerlund, M., & Rajala, R. (2014). Effective Digital Channel Marketing for Cybersecurity Solutions. Technology Innovation Management Review, 4(10), 22–32.

Wilson, M., McDonald, S., Button, D., & McGarry, K. (2023). It Won't Happen to Me: Surveying SME Attitudes to Cyber-security. Journal of Computer Information Systems, 63(2), 397–409. https://doi.org/10.1080/08874417.2022.2067791

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2020). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. Journal of Computer Information Systems, 62(1), 1–17. https://doi.org/10.1080/08874417.2020.1712269