Volume: 9 Issues: 66 [September, 2024] pp. 640 - 650
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: www.jised.com
DOI: 10.55573/JISED.096652

INFORMATION SECURITY BEHAVIOR AMONG MALAYSIAN SMES: PHISHING, CYBERSECURITY INCIDENT, HUMAN FACTORS AND RISK MITIGATION

Mohamad Syauqi Mohamad Arifin[1] [*]
Mohamad Rahimi Mohamad Rosman[1]
Salliza Md Radzi[1]
Nur Ainatul Mardiah Mat Nawi[1]
Noor Azreen Alimin[1]

[1] College of Computing, Informatics and Mathematics, Universiti Teknologi MARA, Kelantan, Malaysia
[*] Correspondence: mohdsyauqi@uitm.edu.my.

Article history
Received date : 15-8-2024
Revised date : 16-8-2024
Accepted date : 7-9-2024
Published date : 15-10-2024

To cite this document:
Mohamad Arifin, M. R., Mohamad Rosman, N. N. I., Md Radzi, A. I., Mat Nawi, N. A. M., & Alimin, N. A. (2024). Information security behavior among Malaysian SMEs: Phishing, cybersecurity incident, human factors and risk mitigation. *Journal of Islamic, Social, Economics and Development (JISED)*, 9 (66), 640 – 650.

Abstract: *Information security concerns is one of the most important issues faced by Malaysian Small and Medium Enterprise (SMEs). The rise of cybersecurity threat especially in digital environment caused losses to Malaysian's SMEs and preventing nationwide digitalization efforts. Thus, more efforts, services, and campaign are needed to revive the digital platform among Malaysian's SMEs. Three important issues faced by Malaysian's SMEs are related to phishing, cybersecurity incidents, and human factors. Therefore, this paper study the literature on the underlying cause of information security behavior among Malaysian's SMEs – and subsequently underlying the future research direction..*

Keywords: *Cybersecurity, phishing, incidents, human security behavior.*

Volume: 9 Issues: 66 [September, 2024] pp. 640 - 650
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: www.jised.com
DOI: 10.55573/JISED.096652

Introduction

Information security is a critical concern for businesses worldwide, particularly for small and medium-sized enterprises (SMEs) operating in Malaysia. In today's digital landscape, where technological advancements offer unprecedented opportunities for growth and efficiency, they also present significant risks. Malaysian SMEs, like their counterparts globally, face an array of cyber threats ranging from phishing attacks to data breaches, which can have devastating consequences for their operations, finances, and reputation. The importance of information security in Malaysian SMEs cannot be overstated. These businesses form the backbone of the Malaysian economy, contributing significantly to employment, innovation, and economic growth. However, their size and resource constraints often make them attractive targets for cybercriminals seeking to exploit vulnerabilities in their systems and processes. Unlike large enterprises with dedicated cybersecurity teams and substantial budgets, SMEs may lack the necessary expertise and resources to adequately protect themselves against evolving cyber threats (Bada & Nurse, 2019; Wallang et al., 2022).

Moreover, in an increasingly interconnected digital ecosystem, Malaysian SMEs frequently interact with larger organizations, government agencies, and international partners, further amplifying the potential impact of security breaches. A single cybersecurity incident can disrupt supply chains, compromise sensitive data, and erode customer trust, leading to financial losses and legal liabilities (BerkmanTech, 2023; QIC, 2023). Against this backdrop, understanding the importance of information security in Malaysian SMEs becomes paramount. Beyond the immediate financial implications, effective information security practices can safeguard the long-term viability and competitiveness of these businesses. By proactively addressing cyber risks, SMEs can enhance their resilience, protect their intellectual property, and foster trust among customers, partners, and stakeholders (Antunes et al., 2021; Wallang et al., 2022).

Today, the rapid digitization of business operations has ushered in a new era of opportunities and challenges for SMEs in Malaysia. With the increasing reliance on digital technologies, SMEs are exposed to a myriad of cybersecurity threats that can disrupt operations, compromise sensitive information, and undermine business continuity. Despite the growing emphasis on information security, Malaysian SMEs continue to grapple with significant vulnerabilities stemming from factors such as resource constraints, lack of expertise, and evolving cyber threats (Wallang et al., 2022). The escalating threats of phishing, cybersecurity incidents, and human factors pose pressing challenges for Malaysian SMEs. Phishing attacks, characterized by deceptive tactics aimed at obtaining sensitive information, exploit human vulnerabilities and pose a significant risk to SMEs (Back & Guerette, 2021). Furthermore, the frequency and severity of cybersecurity incidents, including data breaches and malware infections, continue to rise, causing financial losses and reputational damage. Moreover, human factors, such as employee negligence and susceptibility to social engineering tactics, further exacerbate the vulnerability of Malaysian SMEs to cyber threats (Kumah, 2022).

Furthermore, as Malaysia continues to position itself as a regional hub for innovation and entrepreneurship, the government has recognized the significance of cybersecurity for the nation's digital economy. Initiatives such as the National Cyber Security Policy and various capacity-building programs aim to strengthen the cybersecurity posture of Malaysian SMEs, empowering them to navigate the evolving threat landscape more effectively. In this context, this research paper aims to provide a comprehensive overview of information security behavior among Malaysian SMEs, focusing specifically on phishing, cybersecurity incidents, human factors, and risk mitigation strategies. By analyzing current practices and challenges, this study

Volume: 9 Issues: 66 [September, 2024] pp. 640 - 650
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: www.jised.com
DOI: 10.55573/JISED.096652

seeks to inform policymakers, industry stakeholders, and SME owners/managers about the importance of prioritizing information security and implementing robust measures to protect their businesses in an increasingly digitized world. Through a descriptive analysis, this study seeks to inform policy development, raise awareness, and empower Malaysian SMEs to strengthen their resilience against evolving cyber threats.

Literature Review

Information Security Definition

Information security is a foundational concept in the realm of cybersecurity, encompassing a set of principles, practices, and technologies aimed at protecting sensitive data and ensuring the confidentiality, integrity, and availability of information assets (Vacca, 2012). Various definitions of information security exist within the literature, reflecting its multifaceted nature and evolving landscape. At its core, information security is concerned with safeguarding information from unauthorized access, disclosure, alteration, or destruction. This includes not only digital data stored in electronic systems but also physical records, intellectual property, and other forms of sensitive information. Effective information security measures seek to mitigate risks associated with potential threats, including cyber-attacks, insider threats, and environmental hazards.

Information security is a multifaceted concept that encompasses a range of principles, practices, and technologies aimed at protecting sensitive data and ensuring the confidentiality, integrity, and availability of information assets (ISO/IEC 27000:2018). At its core, information security is concerned with mitigating risks associated with unauthorized access, disclosure, alteration, or destruction of information, whether stored in electronic systems or in physical form. According to the International Organization for Standardization (ISO), information security is defined as "the preservation of confidentiality, integrity, and availability of information" (ISO/IEC 27000:2018). This definition highlights three fundamental objectives (Dalal et al., 2022):

1. Confidentiality: This refers to the protection of sensitive information from unauthorized access or disclosure. Confidentiality measures ensure that only authorized individuals or entities have access to specific information, thereby preventing unauthorized parties from obtaining sensitive data.
2. Integrity: Integrity involves maintaining the accuracy, reliability, and trustworthiness of information throughout its lifecycle. Integrity measures ensure that information remains unaltered and is protected against unauthorized modifications, deletions, or tampering.
3. Availability: Availability pertains to ensuring timely access to information by authorized users whenever needed. Availability measures safeguard against disruptions or downtime that could prevent users from accessing critical information, thereby ensuring uninterrupted business operations.

In addition to these core objectives, information security encompasses various components, including technical controls, organizational policies and procedures, and awareness initiatives. Technical controls, such as access controls, encryption mechanisms, and intrusion detection systems, are implemented to protect digital assets from cyber threats (Whitman & Mattord, 2017). Organizational practices, such as risk assessments, incident response plans, and employee training programs, are essential for establishing a culture of security awareness and accountability within an organization (Avgerou, 2001).

Volume: 9 Issues: 66 [September, 2024] pp. 640 - 650
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: www.jised.com
DOI: 10.55573/JISED.096652

Moreover, human factors play a critical role in information security, as employees' behaviors and actions can significantly impact the effectiveness of security measures. Therefore, fostering a security-conscious culture and promoting awareness of cybersecurity best practices among employees are crucial aspects of information security management (Herath & Rao, 2009; Hooper & Blunt, 2020). In summary, information security is a comprehensive discipline that encompasses technical, organizational, and human aspects aimed at safeguarding sensitive information and ensuring the confidentiality, integrity, and availability of information assets in the face of evolving cyber threats. By adopting holistic approaches that integrate technical controls, organizational practices, and awareness initiatives, organizations can effectively mitigate risks and protect their digital assets from potential threats.

Small and medium-sized enterprises (SMEs) in Malaysia

Small and Medium-sized Enterprises (SMEs) in Malaysia represent a vital segment of the economy, contributing significantly to employment, innovation, and economic growth. According to the statistics from the Department of Statistics Malaysia (DoSM), SMEs accounted for 97.4% of overall establishments in Malaysia in 2022, showing a slight decrease from the previous figure. This data indicates that SMEs continue to play a significant role in the Malaysian business landscape, with the services sector consistently representing more than 80% of all MSMEs. Additionally, the majority of MSMEs in Malaysia are microenterprises, comprising 78.7% of total MSMEs, followed by small-sized firms at 19.7% and medium-sized firms at 1.6% (cleartax, 2024; OECD iLibrary, 2022). Despite their economic significance, SMEs often face challenges in managing cybersecurity effectively due to factors such as limited resources, expertise, and awareness.

Previous study has indicated that SMEs in Malaysia are increasingly targeted by cyber threats, posing significant risks to their operations, financial stability, and reputation. Cyber threats such as phishing, malware infections, ransomware attacks, and data breaches are prevalent among SMEs, highlighting the importance of addressing cybersecurity challenges within this sector (Chetioui et al., 2022; Krombholz et al., 2015). These attacks can result in financial losses, reputational damage, and disruptions to business operations, underscoring the need for effective cybersecurity strategies tailored to the unique needs and constraints of SMEs.

Overview of phishing and its impact on SMEs in Malaysia

Phishing, a prevalent cyber threat, continues to pose significant risks to small and medium-sized enterprises (SMEs) in Malaysia, threatening their operations, financial stability, and reputation. Phishing attacks involve deceptive tactics, such as fraudulent emails or websites, designed to trick individuals into divulging sensitive information like passwords, financial data, or personal details (Tyagi et al., 2023). These attacks often target employees within organizations, exploiting human vulnerabilities to gain unauthorized access to confidential information or infect systems with malware (Alsharnouby et al., 2015). The impact of phishing on SMEs in Malaysia is multifaceted and profound. Firstly, SMEs in Malaysia typically operate with limited resources and may lack dedicated cybersecurity teams, making them prime targets for phishing attacks (Whitman & Mattord, 2017). Without robust security measures in place, SMEs are more susceptible to falling victim to phishing scams, potentially leading to substantial financial losses and operational disruptions.

Moreover, successful phishing attacks can have severe financial consequences for SMEs in Malaysia. Compromised financial data, such as banking credentials or credit card information, can result in fraudulent transactions and financial theft, leading to direct monetary losses for

Volume: 9 Issues: 66 [September, 2024] pp. 640 - 650
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: www.jised.com
DOI: 10.55573/JISED.096652

the affected SMEs (Krombholz et al., 2015). Additionally, the costs associated with mitigating the aftermath of a phishing attack, including incident response, recovery efforts, and legal expenses, can further strain the financial resources of SMEs. Beyond financial implications, phishing attacks can also inflict reputational damage on SMEs in Malaysia. Trust and confidence are paramount in business relationships, and a phishing incident that compromises customer data or exposes sensitive information can erode trust in the affected SME's brand (Dinev & Hart, 2006). The loss of customer trust can have long-term consequences, impacting customer loyalty, brand reputation, and ultimately, the profitability and sustainability of the SME.

Furthermore, phishing attacks can expose SMEs in Malaysia to regulatory and legal risks. The Personal Data Protection Act (PDPA) in Malaysia imposes obligations on organizations to protect the privacy and confidentiality of personal data (Urus et al., 2023). Failure to safeguard sensitive information from phishing attacks can result in regulatory penalties, legal liabilities, and damage to the SME's compliance reputation. To mitigate the impact of phishing attacks, SMEs in Malaysia must prioritize cybersecurity and adopt proactive measures to enhance their resilience. This includes investing in employee training and awareness programs to educate staff about the risks of phishing and how to identify and report suspicious emails (Mentzas et al., 2007). Additionally, SMEs can implement robust email filtering and anti-phishing technologies to detect and block malicious messages before they reach employees' inboxes (Whitman & Mattord, 2017). By taking proactive steps to strengthen their cybersecurity defenses, SMEs in Malaysia can better protect their sensitive information, preserve their reputation, and safeguard their business operations against the evolving threat of phishing.

Affecting of cybersecurity incidents on SMEs in Malaysia

Cybersecurity incidents pose significant threats to small and medium-sized enterprises (SMEs) in Malaysia, jeopardizing their operations, financial stability, and reputation. These incidents encompass a wide range of malicious activities perpetrated by cybercriminals with the intent to exploit vulnerabilities in SMEs' digital infrastructure. Understanding the types of cybersecurity incidents that commonly affect SMEs in Malaysia is crucial for implementing effective risk mitigation strategies and safeguarding against potential threats. One prevalent type of cybersecurity incident affecting SMEs in Malaysia is malware infections. Malware, a broad category of malicious software, includes viruses, worms, ransomware, and Trojans, among others. Malware infections can occur through various vectors, such as malicious email attachments, compromised websites, or USB drives. Once infiltrated, malware can disrupt business operations, steal sensitive data, or hold systems hostage for ransom, causing financial losses and reputational damage to SMEs (Alahmari & Duncan, 2020).

Another significant cybersecurity threat to SMEs in Malaysia is phishing attacks. Phishing involves the use of deceptive tactics, such as fraudulent emails or websites, to trick individuals into divulging sensitive information or clicking on malicious links. Phishing attacks often target employees within SMEs, exploiting human vulnerabilities to gain unauthorized access to confidential data or compromise systems with malware. Successful phishing attacks can lead to data breaches, financial fraud, or unauthorized access to corporate networks, posing serious risks to SMEs' security and integrity (Whitman & Mattord, 2017). Ransomware attacks represent another critical cybersecurity incident impacting SMEs in Malaysia. Ransomware is a type of malicious software designed to encrypt files or lock users out of their systems until a ransom is paid. SMEs are particularly vulnerable to ransomware attacks due to their limited resources and cybersecurity defenses. A successful ransomware attack can disrupt business

Volume: 9 Issues: 66 [September, 2024] pp. 640 - 650
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: www.jised.com
DOI: 10.55573/JISED.096652

operations, compromise sensitive data, and result in financial extortion, posing significant challenges for SMEs' recovery and continuity efforts (Cheng et al., 2017).

Additionally, data breaches pose significant risks to SMEs in Malaysia, exposing sensitive information such as customer data, financial records, or intellectual property to unauthorized access or disclosure. Data breaches can occur due to various factors, including weak passwords, unsecured databases, or insider threats. The consequences of a data breach can be severe, including financial penalties, legal liabilities, and reputational damage, making it imperative for SMEs to prioritize data protection and cybersecurity measures (Tyagi et al., 2023). In conclusion, SMEs in Malaysia face a multitude of cybersecurity incidents that threaten their security, operations, and reputation. Malware infections, phishing attacks, ransomware incidents, and data breaches are among the most prevalent threats impacting SMEs in Malaysia. Understanding the nature and impact of these cybersecurity incidents is essential for SMEs to implement robust security measures, raise awareness among employees, and mitigate the risks posed by cyber threats.

The Influence of human factors on information security behavior

The influence of human factors on information security behavior is a critical aspect of cybersecurity management within organizations, including small and medium-sized enterprises (SMEs). Human factors encompass a wide range of psychological, social, and organizational elements that shape individuals' attitudes, beliefs, and behaviors regarding information security practices. Understanding how human factors influence information security behavior is essential for developing effective strategies to mitigate risks and enhance cybersecurity resilience within SMEs. One significant human factor influencing information security behavior is employee awareness and education. Research suggests that employees' level of awareness and knowledge about cybersecurity threats directly impact their adherence to security policies and practices (Mentzas et al., 2007). Adequate training and educational programs can empower employees to recognize potential security risks, such as phishing attacks or social engineering tactics, and take appropriate preventive measures to mitigate them (Herath & Rao, 2009).

Moreover, individual attitudes and perceptions towards security policies and practices play a crucial role in shaping information security behavior within SMEs. Employees' perceptions of the relevance, effectiveness, and usability of security measures can influence their willingness to comply with organizational security policies (Dhillon & Backhouse, 2001). Positive attitudes towards security, coupled with a perceived sense of personal responsibility for protecting sensitive information, are associated with higher levels of security compliance and adherence among employees. Organizational culture also significantly impacts information security behavior within SMEs. A security-conscious culture that prioritizes and values cybersecurity awareness, accountability, and proactive risk management fosters a supportive environment for promoting information security practices (Chen et al., 2012). Conversely, organizational cultures characterized by lax attitudes towards security, complacency, or resistance to change may hinder employees' willingness to engage in secure behaviors and adhere to security policies.

Furthermore, Social influence and peer pressure can further shape information security behavior within SMEs. Research suggests that employees' behaviors are often influenced by their social networks, including colleagues, supervisors, and peers (Gwebu et al., 2020; Warkentin et al., 2011). Positive social norms that promote security-conscious behaviors, such as reporting

Volume: 9 Issues: 66 [September, 2024] pp. 640 - 650
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: www.jised.com
DOI: 10.55573/JISED.096652

suspicious activities or adhering to password policies, can reinforce desired security practices within SMEs. Also, cognitive biases and decision-making heuristics may affect individuals' information security behavior, leading to deviations from established security protocols. Common cognitive biases, such as overconfidence, confirmation bias, or availability heuristic, can lead employees to underestimate risks or overlook potential threats, thereby compromising security (Whitman & Mattord, 2017). Understanding and addressing these cognitive biases through targeted interventions and awareness programs are essential for promoting more informed and secure decision-making among employees.

Therefore, the influence of human factors on information security behavior within SMEs is multifaceted and complex, encompassing employee awareness, attitudes, organizational culture, social influence, and cognitive biases. Recognizing the interplay between these factors is crucial for developing holistic approaches to cybersecurity management that address both technical and human aspects of security. By fostering a security-conscious culture, providing ongoing education and training, and addressing cognitive biases, SMEs can empower their employees to become active participants in safeguarding sensitive information and mitigating cybersecurity risks effectively.

The influence of trust, belief and subjective norm on Information Security Behavior

The influence of trust, belief, and subjective norms on information security behavior is a critical aspect of cybersecurity research, shedding light on the psychological and social factors that shape individuals' attitudes and actions regarding security practices within organizations. Trust refers to individuals' confidence in the reliability, integrity, and confidentiality of organizational systems and processes, while belief reflects individuals' perceptions of the effectiveness and importance of security measures (Chen & Zahedi, 2016; Xu & Mahenthiran, 2021). Subjective norms encompass social influences and peer pressure that influence individuals' perceptions of what is considered appropriate or acceptable behavior within their social context (Ajzen, 1991; Gupta, 2021).

Research indicates that trust plays a pivotal role in influencing information security behavior among employees within organizations. Individuals who trust in the security of organizational systems and management are more likely to comply with security policies, share sensitive information, and engage in secure behaviors (Dinev & Hart, 2006). Trust in organizational leadership, colleagues, and the effectiveness of security measures fosters a sense of security and confidence among employees, contributing to a culture of security awareness and compliance. Beliefs about the importance and effectiveness of security measures also influence information security behavior. Employees' perceptions of the severity and likelihood of security threats, as well as the efficacy of security controls and protocols, shape their willingness to adopt and adhere to security practices (Whitman & Mattord, 2017). Positive beliefs regarding the benefits of security measures, such as protecting sensitive information, preventing data breaches, and preserving organizational reputation, motivate employees to engage in secure behaviors and support organizational security initiatives. Moreover, subjective norms exert a significant influence on information security behavior within organizations. Social influences from peers, supervisors, and organizational culture shape individuals' perceptions of what constitutes appropriate or acceptable behavior regarding security practices (Guo et al., 2022; Warkentin et al., 2011). Positive social norms that promote security-conscious behaviors, such as reporting suspicious activities, adhering to security policies, and sharing security-related

Volume: 9 Issues: 66 [September, 2024] pp. 640 - 650
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: www.jised.com
DOI: 10.55573/JISED.096652

information, reinforce desired security practices and contribute to a collective sense of responsibility for cybersecurity within the organization.

The interplay between trust, belief, and subjective norms underscores the importance of addressing both individual and social factors in promoting information security behavior. Organizations can cultivate trust by demonstrating transparency, competence, and commitment to security initiatives, thereby fostering a supportive environment for security awareness and compliance (Li et al., 2021; Siponen & Vance, 2010). Additionally, organizations can leverage positive beliefs about the benefits of security measures and cultivate social norms that encourage security-conscious behaviors through training, communication, and reinforcement of security policies (Guo et al., 2022; Warkentin et al., 2011).

Therefore, the influence of trust, belief, and subjective norms on information security behavior highlights the complex interplay between individual perceptions, social influences, and organizational culture within the context of cybersecurity. Understanding and addressing these psychological and social factors are essential for developing effective strategies to promote security awareness, compliance, and resilience within organizations.

Conclusion

The aim of this study is to identify related literature on phishing, security incidents and security human behaviour in the context of Malaysian's SMEs. Subsequently, several variables were identified as a predictor for further research. Based on the literature survey, our next effort is to properly investigate the depth and current level of information security awareness and behaviour among Malaysian's SMEs. In order to proceed with further research, an instrument will be developed by adopting previous instruments that are related to the purpose of the study.

Acknowledgments

The authors would like to thank the financial support received from Universiti Teknologi MARA Kelantan Branch, Malaysia under Internal Grant 600-TNCPI 5/3/DDN (03) (012/2022).

Volume: 9 Issues: 66 [September, 2024] pp. 640 - 650
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: www.jised.com
DOI: 10.55573/JISED.096652

References

Ajzen, I. (1991). The theory of planned behavior. *Organizational behavior and human decision processes*, *50*(2), 179-211. https://doi.org/10.1016/0749-5978(91)90020-T

Alahmari, A., & Duncan, B. (2020). *Cybersecurity Risk Management in Small and Medium-Sized Enterprises: A Systematic Review of Recent Evidence*. https://doi.org/10.1109/CyberSA49311.2020.9139638

Alsharnouby, M., Alaca, F., & Chiasson, S. (2015). Why phishing still works: User strategies for combating phishing attacks. *International Journal of Human-Computer Studies*, *82*, 69-82. https://doi.org/10.1016/j.ijhcs.2015.05.005

Antunes, M., Maximiano, M., Gomes, R., & Pinto, D. (2021). Information security and cybersecurity management: A case study with SMEs in Portugal. *Journal of Cybersecurity and Privacy*, *1*(2), 219-238. https://doi.org/10.3390/jcp1020012

Avgerou, C. (2001). The significance of context in information systems and organizational change. *Information systems journal*, *11*(1), 43-63. https://doi.org/10.1046/j.1365-2575.2001.00095.x

Back, S., & Guerette, R. T. (2021). Cyber place management and crime prevention: the effectiveness of cybersecurity awareness training against phishing attacks. *Journal of contemporary criminal justice*, *37*(3), 427-451. https://doi.org/10.1177/10439862211001628

Bada, M., & Nurse, J. R. (2019). Developing cybersecurity education and awareness programmes for small-and medium-sized enterprises (SMEs). *Information & Computer Security*, *27*(3), 393-410. https://doi.org/10.1108/ICS-07-2018-0080

BerkmanTech. (2023). *Understanding the importance of cybersecurity in small business*. BerkmanTech. Retrieved 3rd May from https://berkmantech.com/understanding-the-importance-of-cybersecurity-in-small-business/

Chen, Y., Ramamurthy, K., & Wen, K.-W. (2012). Organizations' information security policy compliance: Stick or carrot approach? *Journal of Management Information Systems*, *29*(3), 157-188. https://doi.org/10.2753/MIS0742-1222290305

Chen, Y., & Zahedi, F. M. (2016). Individuals' internet security perceptions and behaviors. *MIS quarterly*, *40*(1), 205-222. https://doi.org/10.25300/MISQ/2016/40.1.09

Cheng, L., Liu, F., & Yao, D. (2017). Enterprise data breach: Causes, challenges, prevention, and future directions. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, *7*(5), e1211. https://doi.org/10.1002/widm.1211

Chetioui, K., Bah, B., Alami, A. O., & Bahnasse, A. (2022). Overview of social engineering attacks on social networks. *Procedia Computer Science*, *198*, 656-661. https://doi.org/10.1016/j.procs.2021.12.302

cleartax. (2024). *The essential guide for SMEs in Malaysia*. ClearTax. https://www.cleartax.com/my/en/sme-malaysia

Dalal, R. S., Howard, D. J., Bennett, R. J., Posey, C., Zaccaro, S. J., & Brummel, B. J. (2022). Organizational science and cybersecurity: abundant opportunities for research at the interface. *Journal of business and psychology*, *37*(1), 1-29. https://doi.org/10.1007%2Fs10869-021-09732-9

Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: towards socio-organizational perspectives. *Information systems journal*, *11*(2), 127-153. https://doi.org/10.1046/j.1365-2575.2001.00099.x

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information systems research*, *17*(1), 61-80. https://doi.org/10.1287/isre.1060.0080

Guo, Y., Wang, X., & Wang, C. (2022). Impact of privacy policy content on perceived effectiveness of privacy policy: the role of vulnerability, benevolence and privacy concern.

Volume: 9 Issues: 66 [September, 2024] pp. 640 - 650
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: www.jised.com
DOI: 10.55573/JISED.096652

Journal of Enterprise Information Management, *35*(3), 774-795. https://doi.org/10.1108/JEIM-12-2020-0481

Gupta, V. (2021). Green purchase intention: Impact of subjective norms and perceived behavioural control. *MANTHAN: Journal of Commerce and Management*, *8*(1), 116-134. https://doi.org/10.17492/jpi.manthan.v8i1.812107

Gwebu, K. L., Wang, J., & Hu, M. Y. (2020). Information security policy noncompliance: An integrative social influence model. *Information systems journal*, *30*(2), 220-269. https://doi.org/10.1111/isj.12257

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of information systems*, *18*, 106-125. https://doi.org/10.1057/ejis.2009.6

Hooper, V., & Blunt, C. (2020). Factors influencing the information security behaviour of IT employees. *Behaviour & Information Technology*, *39*(8), 862-874. https://doi.org/10.1080/0144929X.2019.1623322

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and applications*, *22*, 113-122. https://doi.org/10.1016/j.jisa.2014.09.005

Kumah, P. (2022). The role of human resource management in enhancing organizational information systems security. In *Research Anthology on Human Resource Practices for the Modern Workforce* (pp. 1251-1277). IGI Global. https://doi.org/10.4018/978-1-6684-3873-2.ch065

Li, H., Luo, X. R., & Chen, Y. (2021). Understanding information security policy violation from a situational action perspective. *Journal of the Association for Information Systems*, *22*(3), 739-772. https://doi.org/10.17705/1jais.00678

Mentzas, G., Kafentzis, K., & Georgolios, P. (2007). Knowledge services on the semantic web. *Communications of the ACM*, *50*(10), 53-58. https://doi.org/10.1145/1290958.1290962

OECD iLibrary. (2022). *Financing SMEs and entrepreneurs 2022: An OECD scoreboard*. OECD. https://www.oecd-ilibrary.org/sites/3bc2915c-en/index.html?itemId=%2Fcontent%2Fcomponent%2F3bc2915c-en

QIC. (2023). *Cyber attacks: The silent killer of small businesses*. Digital Venture Partners. Retrieved 3rd May from https://qic-digitalventures.com/2023/12/11/cyber-attacks-the-silent-killer-of-small-businesses/

Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS quarterly*, 487-502. https://doi.org/10.2307/25750688

Tyagi, S., Tyagi, D., Dutta, P., & Dubey, D. (2023). *Next Generation Phishing Detection and Prevention System using Machine Learning*. https://doi.org/10.1109/ICAISC56366.2023.10085529

Urus, S. T., Othman, I. W., Rasit, Z. A., Bakar, N. A., & Nazri, S. N. F. S. M. (2023). Beyond the hype of big data analytics deployment: Conceptualization and challenges epistemology. *Business and Economic Research*, *13*(2), 74-111. https://doi.org/10.5296/ber.v13i2.20807

Vacca, J. R. (2012). *Computer and information security handbook*. Newnes. https://perpus.univpancasila.ac.id/repository/EBUPT200101.pdf

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

Warkentin, M., Johnston, A. C., & Shropshire, J. (2011). The influence of the informal social learning environment on information privacy policy compliance efficacy and intention. *European Journal of information systems*, *20*, 267-284.

Volume: 9 Issues: 66 [September, 2024] pp. 640 - 650
Journal of Islamic, Social, Economics and Development (JISED)
eISSN: 0128-1755
Journal website: www.jised.com
DOI: 10.55573/JISED.096652

https://doi.org/10.1057/ejis.2010.72

Whitman, M. E., & Mattord, H. J. (2017). *Principles of information security* (6th ed.). Cengage Learning. https://g.co/kgs/5DKVo5x

Xu, H., & Mahenthiran, S. (2021). Users' perception of cybersecurity, trust and cloud computing providers' performance. *Information & Computer Security*, *29*(5), 816-835. https://doi.org/10.1108/ICS-09-2020-0153