Advances in Humanities and Contemporary Studies Vol. 2 No. 1 (2021) 192-210
© Universiti Tun Hussein Onn Malaysia Publisher's Office

AHCS

Homepage: http://publisher.uthm.edu.my/periodicals/index.php/ahcs
e-ISSN : 2773-4781

Evaluation of Information Security Awareness on Digital Marketing (Case Study of MSME in Indonesia)

Ahmad Zamsuri[1]*, Wenni Syafitri[2], Eddis Syahputra Pane[3]

[1]Informatics Engineering, Faculty of Computer Science, Lancang Kuning University, Riau, INDONESIA
[2]Informatics Engineering, Faculty of Computer Science, Lancang Kuning University, Riau, INDONESIA
[3]Information Systems, Faculty of Computer Science, Lancang Kuning University, Riau, INDONESIA

* ahmadzamsuri@unilak.ac.id

DOI: https://doi.org/10.30880/ahcs.2021.02.01.020
Received 05 April 2021; Accepted 28 May 2021; Available online 25 June 2021

Abstract: Digital marketing allows more intensive interaction, especially getting personal information. The mechanism of digital marketing on social media is also experiencing evolution, like on Facebook. Facebook is the choice of companies and service providers, both large and small, as an advertising medium. This is because they quickly get customers. Ads will be displayed on the customer's Facebook homepage. This ease will pose many threats in the future. Therefore, the formulation of this research is how to evaluate information security awareness in digital marketing, especially at MSME. This study evaluates MSME in Indonesia but is constrained by the number of MSME participating. There were 384 MSME needed, but only 17 were collected—data processing using these data resulted in a good test on reliability, validity, and normality. When assessing the validity, only a few variables are invalid, such as K15, K17, K9, K13, K1, K2, A12, A1, A2, B2, B3, B4, and B14. Overall valid variable items are 79.4%. In contrast, the reliability of each variable K, A, and B is dependable. However, for the data normality test, only the Attitude (A) variable has not been standard.

Keywords: Attitude, Behaviour, HAIS-Q, Knowledge

1. Introduction

The development of social media in the past few years has increased rapidly along with the high level of penetration of social media usage. Facebook social media penetration is 63.03%, Pinterest 14.23%, YouTube 9.66%, Twitter 8.29%, Instagram 2.16% and Tumblr 0.91%. based on the page quoted from the gs.statcounter.com website. The high level of penetration will certainly cause various

**Corresponding author: ahmadzamsuri@unilak.ac.id* information security threats, such as phishing, identity theft, and so on. On the other hand, a high level of penetration will also increase the digital market. The use of advertising by social media includes user information such as hobbies, status updates, comments, search keywords, and others (Gupta et al., 2018).

Therefore, an evaluation of the user's awareness of personal information is very much needed. According to (Bibi et al., 2017), respondents have an elevated level of concern for privacy but a lack of knowledge about information leakage. Related research also includes social media user awareness assessments such as public risk perceptions related to security and privacy on social media and identifying perceived risk factors and pre- warning behavior when using Facebook (van Schaik et al., 2018), analysis of social networks viewed from aspects level of awareness and security policy (Lopes & Pereira, 2017), Trust and Security influence user desires on social networks (Sriratanaviriyakul et al., 2017). Factors of privacy concerns, trustworthiness, the influence of risk beliefs, and the competitiveness of these three factors (Menard & Sharma, 2017). Behavioral intention factors influence Behavioral factors. The apathetic factor does not affect the attitude factor, while the Perception Behavior Control factor influences Social Trust. Perceived Behavior Control Factors do not affect Behavior, and Social Trust does not affect Behavioral Intentions (Foltz et al., 2016). No Significant influence between perceived security factors and perceived privacy and perceived security. Also, sharing information and developing new relationships have negligible effect (Almadhoun et al., 2011).

Based on these problems, an evaluation is needed to anticipate violations of social network security. Limited access to social media allows limited research opportunities; this is because of the policy of supporting user privacy. Therefore, the focus of research is directed at how users can utilize social media to avoid existing threats. This study uses a Hais-Q evaluation tool (Parsons et al., 2017) and measurement of information security awareness levels (Kruger & Kearney, 2006).

Privacy has become something that cannot be resolved by some earlier studies, especially on digital marketing. Many researchers have explored privacy on social media. However, it is limited by limited information because the system sets standards for user privacy. Security standards will no doubt bring latest problems, especially in privacy. Some time ago, Facebook provided data to Cambridge Analytica (Palos- Sanchez et al., 2019). Does the user have an attitude of awareness towards the data after the event?

Case study research is Micro, Small, and Medium Enterprises (MSMEs). Micro, Small, and Medium Enterprises (MSMEs) are among the drivers of the country's economic progress, especially Indonesia (Merdeka, 2018). MSMEs have also succeeded in reducing unemployment (Kompas, 2016, 2017). Therefore, the Government pays special attention to increasing the growth of MSMEs, such as tax relief (Apip, 2018), seminars, or workshops (Directorate General of Learning and Student Affairs, 2019; Kominfo, 2017) and others. The selection of this case study is due to several previous studies in Indonesia, mostly in the Government, Private and Education sectors such as the evaluation of information security awareness of Makassar city government employees (Amin, 2014), bank x employees in Bandung (Islami et al., 2016), financial service authority employees (Natasia, 2018), the ministry of communication and informatics as well as the Directorate General of Resources and Equipment of Post and Information Technology (Puspitaningrum et al., 2018), Sandi Negara High School (Jumiati et al., 2011), high school students equals Jabodetabek (Maulidha, 2018), and Amikom University Yogyakarta (Destya, 2018). However, no research discusses information security awareness in MSME. Digital marketing allows more intensive interaction, especially getting personal information. The mechanism of digital marketing on social media is also experiencing evolution, like on Facebook. Facebook is the choice of companies and service providers, both large and small, as advertising media (Tran, 2017). This is because they quickly get customers. After all, ads will be displayed on the customer's Facebook homepage. Young man This day will pose many threats in the future. Therefore, the formulation of this research is how to evaluate information security awareness in digital marketing, especially at SMEs?

The purpose of this study is:

1. Knowing the results of evaluating information security awareness by digital marketing users on social media.
2. Providing recommendations when interacting on social media for digital marketing.

2. Material and Method

2.1 Information Security Awareness

There is very little information awareness research at MSMEs, mainly the focus on digital marketing. Several studies in Indonesia on information security awareness were carried out on Makassar city government employees (Amin, 2014), and this study successfully identified information security awareness at a moderate level using the Multiple Criteria Decision Analysis (MCDA) method. The study (Islami et al., 2016) used interviews and survey methods based on the Guidelines for the Implementation of Information Security Governance for Public Service Providers for bank x employees in the city of Bandung. The average bank employee has information awareness, but several aspects must be improved again (Islami et al., 2016). Research (Natasia, 2018) evaluates information awareness on Financial Services Authority (OJK) employees using the Knowledge, Attitude, Behavior (KAB) model. The model succeeded in identifying the level of information security awareness of OJK employees, which is at a reasonably good level but has several improvements that must be implemented, such as internet use, incident reporting, and remote work (Natasia, 2018). The use of the National

Institute of Standards and Technology (NIST) standard SP800-100 as an evaluation of information security issues at the Sandi Negara High School (Jumiati et al., 2011). the use of NIST SP800-100 successfully evaluated information awareness at the School (Jumiati et al., 2011).

Very little research on information security awareness on digital marketing by MSMEs. Research is only about cybersecurity at MSMEs, for example, the collaboration of ISO / IEC 27001 and the Analytic Hierarchy Process (AHP) for information security management (Kaušpadienė & Ramanauskaitė, 2019). Review of cybersecurity at SMEs in the era of the Internet of Things (IoT) (Kasl, 2018). Cybersecurity at MSME is influenced by five internal factors, namely budget, lack of management support, IT complexity and legacy systems, attitude toward security, and compliance to regulations. In comparison, external factors are technology groups (security hygiene, software and bandwidth availability and wireless technologies), customer groups (novice users, usage patterns, IT Education, Adversary perspectives and socio-cultural challenges) and pressures and institutions (coercive, normative and mimetic) (Kabanda et al., 2018).

2.2 Electronic Word-of-Mouth (eWOM) in Digital Marketing

eWOM is one of the instruments used by marketing, especially at this time, which has evolved due to the internet. EWOM platforms have sprung up to accommodate the internet, such as blogs, discussion forums, review sites, shopping sites, and social media (Erkan & Evans, 2016). Social media is the most popular platform for users because it allows users to communicate with each other with their networks. EWOM research has been extensively researched on social media such as Facebook, WeChat, Instagram, Twitter, QQ, and other social media.

Current eWOM research is more about evaluating how users interact with eWOM on social media. Research (Kapoor et al., 2019) uses variable source credibility, brand attitude, message credibility, and intention to purchase. Research (Gvili & Levy, 2018) uses Social Capital variables: Bonding Bridging, Credibility, Channel Type, Attitude toward eWOM, and eWOM Engagement: Receive, Send. Research (Bühler et al., 2017) uses variables of social media stimulus, social media experience, and trust. The study (Aghakhani et al., 2016) used Image Building, Tie Strength, Engagement, Affective Attitude, and Implicit eWOM adoption variables. Research (Hsu et al., 2016) uses Sense of Virtual Community, Normative Influence, Information Influence, Perceived eWOM Review Credibility, and eWOM Review Adoption variables. Research (Wu et al., 2014) uses the variable Product attitude, Intention to purchase, Intention to click, Product type, Friends' involvement with an advertisement, and Ties strength. As well as research (Y. C. Yan et al., 2014) using the variable message source credibility, message appeal, and eWOM response.

Several studies have also done the same thing, namely evaluating eWOM on social media Instagram (Danniswara et al., 2017), Twitter (Chu & Sung, 2015), QQ (Teng et al., 2014), and weChat (Sohaib et al., 2019; Yang, 2019), As well as evaluations on the website and social eWOM (Erkan & Evans, 2016; Wang et al., 2018; Q. Yan et al., 2018). Therefore this study very few evaluates information security awareness in digital marketing but can be related to information security aspects such as several research variables Source and Message Credibility (Kapoor et al., 2019; Teng et al., 2014), Trust (Bühler et al., 2017; Sohaib et al., 2019), Information Quality (Danniswara et al., 2017; Erkan & Evans, 2016), Information Credibility (Erkan & Evans, 2016) and Perceived Credibility (Q. Yan et al., 2018).

2.3 Related Research

Very little information security awareness research on MSMEs like (Bada & Nurse, 2019) conducted an information security awareness review on the Small Medium Enterprise (SME) in the fields of finance, education, communications and technology, health, transportation, real estate, and manufacturing (Bada & Nurse, 2019). (Bada & Nurse, 2019) The London Digital Security Center (LDSC) oversees SME information security awareness through workshops for 3 to 6 months. It is best to (Bada & Nurse, 2019) conduct an evaluation of the existing MSMEs, then only carry out a guard against information security awareness. It aims to make it easier to provide an overview of the problems faced by the SME. Meanwhile, (Lejaka et al., 2019) conducted a review and identified a framework for information security awareness in SMME. (Lejaka et al., 2019) conducted research in South Africa and produced the components needed for cybersecurity awareness research. Therefore, information security awareness research is currently limited to the review and identification of information security awareness in certain cases.

Some studies are more likely to evaluate information awareness, but not at MSMEs such as research (Ahmad et al., 2019) evaluating information security awareness of parents of students in Malaysia. The research is limited to parents of students in public schools, so that it has not been able to provide generalization results for parents of students in Malaysia. However, this research has revealed that parents' information security awareness is of a moderate level.

Some studies also evaluate information security awareness at the university level as conducted by (Gkioulos et al., 2017; Zeki & Hamid, 2016). Respondents (Zeki & Hamid, 2016) are postgraduate students, while (Gkioulos et al., 2017) are students born in 1987-1997. Both studies are equally concerned with aspects of the use of information and communication technology in everyday life. (Zeki & Hamid, 2016) evaluates information security awareness on the use of information systems while (Gkioulos et al., 2017) on the use of mobile devices. (Zeki & Hamid, 2016) and (Gkioulos et al., 2017) did not provide information security awareness levels in their research. So, it is not known what the results of the evaluation of the level of information security awareness in the study.

(Alotaibi et al., 2017) also conduct information security evaluations of people in Saudi Arabia with criteria of age 18 years and above, because they want to focus on how the results of evaluating information security awareness in adults. This research succeeded in identifying the information security awareness of the community, but it was not stated in terms of level.

Some cybersecurity awareness studies are also conducted in Indonesia but not at MSMEs, such as Research (Destya, 2018), conducting a review of the RBS (Risky Behavior Scale) model, CBS (Conservative Behavior Scale), and EOS (Exposure Offense Scale). The research will be applied at Yogyakarta Amikom University to get the results of the review. Research (Akraman et al., 2018) and (ULTA, 2018) conducted an information security awareness evaluation on smartphone users at the general and university level. They use information security awareness measurement scales from (Kruger & Kearney, 2006) and Knowledge, Attitude, and Behavior (KAB) instruments. However, what is different from their research is the findings of the study, namely (Akraman et al., 2018) describing the results of each evaluation on the KAB instrument while (ULTA, 2018) provides information about the effect on each KAB instrument. The KAB instrument successfully found the security awareness of the user's information on the smartphone. However, some studies evaluate information security awareness using instruments from research results (Parsons et al., 2017). (Parsons et al., 2017) said that the Hais-Q instrument had been developed and refined for various populations including students, the general public as well as government and financial institutions. Several studies using Hais-Q are the collaboration of Hais-Q and HEXACO (Maulidha, 2018), a review of ISO 27001 collaboration, our index, and Hais-Q (Budi & Tarigan, 2018) and the collaboration of Hais-Q and Our Index (Puspitaningrum et al., 2018). Based on research (Budi & Tarigan, 2018; Maulidha, 2018; Puspitaningrum et al., 2018), the Hais-Q instrument can provide an overall picture of information security awareness for users.

This study will use the Hais-Q instrument based on recommendations from (Budi & Tarigan, 2018; Maulidha, 2018; Puspitaningrum et al., 2018). Nevertheless, this research is different from (Puspitaningrum et al., 2018), they evaluated information security awareness at the ministry of communication and informatics as well as the Directorate General of Resources and Equipment of Post and Information Technology, while this research was to MSMEs where this case study had no research focused on MSMEs what else in Indonesia. Existing research is still limited to reviewing and monitoring the results of information security awareness training (Bada & Nurse, 2019; Lejaka et al., 2019). Furthermore, the use of information security awareness levels (Kruger & Kearney, 2006) to measure the level of information security awareness at MSMEs.

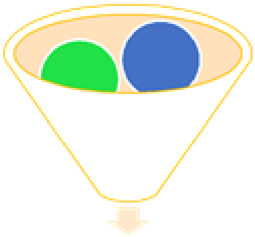

Figure 6. Theoretical Framework

3. Analysis and Discussion

3.1 Demographics of Respondents

This research experienced problems in gathering respondents; we have tried to collect data optimally by distributing questionnaires online. The questionnaire has been distributed on various social media. Karis until now only filled by 17 respondents. The following is a general description of the respondent's profile.

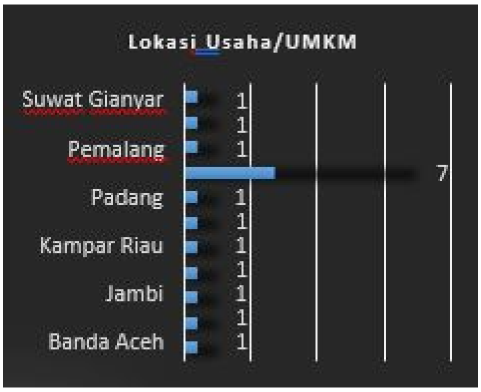

Figure 3. Distribution of MSME locations

The dominant respondents came from the city of Pekanbaru based on Figure 3. Distribution of MSME locations.

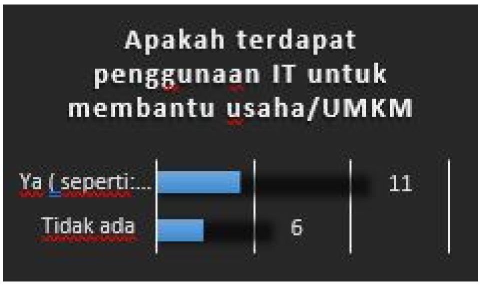

Figure 4. The use of IT in MSMEs

However, the use of IT is beneficial for the efforts of MSMEs based on Figure 4.

Advances in Humanities and Contemporary Studies Vol. 2 No. 1 (2021) 192-210
© Universiti Tun Hussein Onn Malaysia Publisher's Office

AHCS

Homepage: http://publisher.uthm.edu.my/periodicals/index.php/ahcs
e-ISSN : 2773-4781

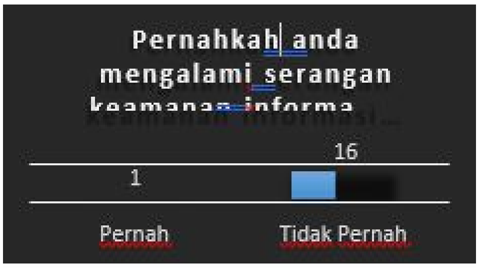

Figure 5. MSMEs are under cyber attack

Based on 17 respondents, only one respondent reported that they were cheated or hacked based on Figure 5.

A. Normality. Normality testing is highly recommended to find out how the distribution of data.

However, the obstacle to this research is getting respondents. The respondents we collected were not optimal, so the normality test was not optimal.

Table 11. Normality test

	Kolmogorov-Smirnov^a			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
K	.171	17	.200*	.923	17	.167
A	.265	17	.003	.835	17	.006
B	.220	17	.029	.865	17	.019

According to Table 4, data normality cannot be achieved in the Attitude (A) variable because the value of p-value / Sig is not more than 0.05.

B. Validity

The validity of this study was tested using Product Moment, so the R table value for the 5% significance level was 0.482. The following is a comparison of the Rtable and Rhitung values.

Table 12. The validity of Knowledge

Knowledge Variable	Sum of Scale	Justification
[K3] Saya Pearson diizinkan Correlat mengklik ion link apapun Sig. (2- dari email tailed) orang yang	.639**	Valid
[K4] Saya Pearson diizinkan Correlat untuk ion membuka Sig. (2- lampiran tailed) email dari pengirim N yang tidak	.628** .007	Valid
[K5] Saya Pearson diizinkan Correlat untuk ion mendownlo Sig. (2- ad file tailed) apapun kedalam komputer kerja, jika file tersebut N dapat membant	.494* .044	Valid
[K6] Saya Pearson diizinkan Correlat memasukka ion n informasi Sig. (2- apa pun di tailed) situs web apa pun jika itu membantu saya N melakukan	.522* .032	Valid

Knowledge Variable	Sum of Scale	Justification
saya posting di media N sosial	17	
[K8] saya Pearson dapat Correlat memposting ion apa yang Sig. (2- saya tailed) inginkan tentang pekerjaan di N media sosial	.665 ** .004 17	Valid
[K9] Saya Pearson diizinkan Correlat mengirim ion file kerja Sig. (2- yang rahasia tailed) melalui jaringan Wi-	.454 .067 17	not Valid
[K10] Hasil Pearson print Correlat dokumen ion rahasia Sig. (2- sama-sama tailed) dapat dibua ng seper ti halnya N dokumen	.660 ** .004 17	Valid
[K11] Saya Pearson diizinkan Correlat meninggalk ion an cetakan Sig. (2- yang berisi tailed) informasi rahasia di N meja saya	.676 ** .003 17	Valid
[K12] Pearson Melaporkan Correlat insiden ion keamanan Sig. (2- adalah tailed)	.589 * .013	Valid

Knowledge Variable	Su m of Scal	Justificat ion
[K13] Perlu Pearson menggunaka Correlat n kombinasi ion huruf, angka Sig. (2- dan simbol tailed) untuk	.477 .053	not Valid
[K14] Saya Pearson tidak Correlat diizinkan ion untuk Sig. (2- mengklik tailed) link apapun	.521 * .032	Valid
[K15] Pearson Sementara Correlat saya sedang ion bekerja, Sig. (2- saya tidak tailed) boleh mengakses situs web N	.378 .135	not Valid
[K16] Saya Pearson harus secara Correlat berkala ion meninjau Sig. (2- pengaturan tailed) privasi di akun media N	.617 **	Valid
[K17] Pearson Ketika Correlat bekerja di ion tempat Sig. (2- umum, saya tailed) harus selalu membawa N	.241 .352	not Valid
[K18] ketika Pearson bekerja Correla t ion pada dokumen	.802 **	Valid

Knowledge Variable	Sum of Scale	Justification
memastikan bahwa orang lain tidak dapat N melihat	17	
[K19] Jika Pearson saya Correlat menemukan ion USB Flash Sig. (2- Drive di tailed) tempat umum, saya tidak harus mencolokka N nnya ke komputer kerja saya.	.703 ** .002	Valid
[K20] jika Pearson saya melihat Correlat seseorang ion bertindak Sig. (2- mencurigak tailed) an di tempat kerja saya, saya harus N	.602 * .010	Valid
[K21] saya Pearson tidak boleh Correlat mengabaika ion n perilaku Sig. (2- keamanan tailed) yang buruk oleh rekan N sejawat saya	.780 ** .000	Valid

Attitude varia ble		Sum of sca le	Justific ation
[A1] Aman Pearso untuk n menggunakan Correla kata sandi tion yang sama Sig. (2- pada akun tailed) media sosial		.39 4	not Valid
[A2] Aman Pearso menggunakan n kata sandi pada Correla akun kerja tion dengan Sig. (2- Pearso		.17 5	not Valid
[A3] Selalu n aman untuk Correla mengklik link tion		.58 1*	Valid
[A4] Tidak ada Pearso hal buruk yang n dapat terjadi Correla jika saya tion mengklik link Sig. (2-		.62 2**	Valid
[A5] Selama Pearso membantu n pekerjaan Correla saya, tidak tion masalah Sig. (2- informasi tailed) apapun yang		.51 6* .03	Valid
[A6] Tidak Pearso masalah jika n saya Correla memposting tion sesuatu di Sig. (2- media sosial tailed)		.61 5** .00	Valid

According to table 5, invalid variables, namely K15, K17, K9, K13, K1, and K2.

Table 13. The validity of Attitude variable

Attitude varia ble			Su m of sca	Just ific atio
[A7] Ketika Pearso bekerja di n sebuah kafe Correla atau ruang tion publik, aman Sig. (2- untuk tailed) meninggalkan laptop saya tanpa pengawasan N selama beberapa			.72 8^{**} .00 1 17	Valid
[A8] Pearso Membuang n hasil cetakan Correla dokumen tion rahasia dengan Sig. (2- memasukkann tailed) ya ke tempat sampah adalah N			.52 6^{*} .03 0 17	Valid
[A9] Jika saya Pearso menemukan n usb flash drive Correla di tempat tion umum, tidak Sig. (2- ada hal buruk tailed) yang dapat terjadi jika saya mencolokkann N ya ke komputer/lapt op kerja saya.			.65 5^{**} .00 4 17	Valid
[A10] Jika Pearso saya n mengabaikan Correla seseorang yang tion bertindak Sig. (2- mencurigakan tailed) di tempat kerja saya, tidak ada hal buruk yang N dapat terjadi			.85 2^{**} .00 0 17	Valid
[A11] tidak ada hal buruk yang akan terjadi jika	Pearso n Correla tion		.79 1^{**}	Valid

Attitude varia ble		Su m of sc	Justific ation
saya Sig. (2- mengabaikan tailed) perilaku keamanan buruk yang N		.00 0	
[A-12] Ide Pearso yang buruk n untuk Correla membagikan tion kata sandi Sig. (2- akun pekerjaan tailed) saya, walaupun N		.31 4 .22 0	not Valid
[A13] Pearso Membuka n lampiran email Correla dari pengirim tion yang tidak Sig. (2- dikenal tailed) memiliki risiko N		.72 6^{**}	Valid
[A14] Pearso Mengunduh/d n ownload file Correla menggunakan tion komputer Sig. (2- kantor saya tailed) memiliki risiko N		.62 8^{**}	Valid
[A15] Pearso Mengakses n sebuah website Correla dari kantor, tion bukan berarti Sig. (2- aman dari tailed) risiko. N		.67 8^{**}	Valid
[A16] Evaluasi Pearso secara berkala n pengaturan Correla privasi di tion media sosial Sig. (2- merupakan ide tailed) yang bagus. N		.73 3^{**}	Valid

AHCS

Homepage: http://publisher.uthm.edu.my/periodicals/index.php/ahcs
e-ISSN : 2773-4781

Attitude variable		Sum of scale	Justification
[A17] Berisiko Pearso memposting n informasi Correla tertentu tion tentang Sig. (2- pekerjaan saya tailed) di media sosial N		.487*	Valid
Pearso [A18] n Mengirimkan Correla file kerja yang tion bersifat rahasia Sig. (2- adalah risiko tailed)		.759**	Valid
N [A19] Pearso Mengakses file n kerja saya Correla yang rahasia di tion laptop ketika Sig. (2- orang lain tailed) dapat melihat		.819** .00	Valid
[A20] Pearso Meninggalkan n cetakan Correla dokumen tion rahasia di meja Sig. (2- semalaman tailed) adalah risiko N		.921**	Valid
[A21] Pearso Mengabaikan n insiden Correla keamanan, tion bahkan jika Sig. (2- saya pikir itu tailed) tidak signifikan N adalah risiko		.807** .00	Valid

Behavior variable	Sum of scale	Justification
[B1] Saya Pearson membagikan Correla kata sandi tion akun Sig. (2- pekerjaan tailed) saya dengan rekan sejawat N	.639** .00	Valid
[B2] Jika Pearson email dari Correla pengirim tion yang tidak Sig. (2- dikenal tailed) terlihat menarik, saya mengklik link N di dalam email tersebut	.314 .220	not Valid
[B3] Saya Pearson mengunduh Correla file apa pun tion ke komputer Sig. (2- kerja saya tailed) yang akan membantu N menyelesaika	.249 .336	not Valid
[B4] Ketika Pearson mengakses Correla internet di tion saya tailed) mengunjungi	.425 .089	not Valid
[B5] Saya Pearson tidak secara Correla teratur tion meninjau Sig. (2- pengaturan tailed) privasi akun media sosial N	.484* .049	Valid
[B6] Saya memposting apa pun yang saya inginkan Pearson Correla tion Sig. (2-	.58 *	Valid

Behavior variable	Sum of scal	Justification
pekerjaan saya di media N	17	
[B7] Ketika Pearson bekerja di Correla tempat tion umum, saya Sig. (2- meninggalka tailed) n laptop saya	.83 ** .00 0	Valid
[B8] Saya Pearson mengirim file Correla kerja yang tion rahasia Sig. (2- menggunakan tailed) jaringan Wi- Fi umum. N	.64 2 1** .00	Valid
[B9] Saya Pearson meninggalka Correla n cetakan tion dokumen Sig. (2- rahasia di tailed) meja saya ketika tidak berada di N	.84 7** .00 0	Valid
[B10] Jika Pearson rekan sejawat Correla mengabaikan tion aturan Sig. (2- keamanan, tailed) saya tidak akan mengambil N	.71 1** .00 1	Valid
[B11] Saya Pearson menggunakan Correla kata sandi tion yang berbeda Sig. (2- untuk akun tailed) media sosial dan pekerjaan N	.49 4* .04 4	Valid
[B12] Saya Pearson menggunakan Correla kombinasi tion	.87 **	Valid

Behavior variable	Sum of scal	Justification
huruf, angka, Sig. (2- dan simbol tailed) dalam kata sandi akun sistem informasi atau aplikasi yang N berkaitan	.00 0	
[B13] Saya Pearson tidak selalu Correla mengklik link tion dalam email Sig. (2- hanya karena tailed) link berasal dari yang saya	.57 6* .01 5	Valid
[B14] Saya Pearson tidak Correla membuka tion lampiran Sig. (2- email jika tailed) pengirimnya seseorang N kenal.	.03 5 .89 4	not Valid
[B15] Saya Pearson menilai Correla keamanan tion situs web Sig. (2- sebelum tailed) memasukkan informasi ke N	.89 9** .00 0	Valid
[B16] Saya Pearson tidak Correla memposting tion apa pun di Sig. (2- media sosial tailed) sebelum mempertimbangkan N konsekuensi	.88 5** .00 0	Valid

Behavior variable	Sum of scal	Justification
pun yang		
[B17] Saya Pearson memastikan Correla bahwa orang tion lain tidak Sig. (2- dapat melihat tailed) layar laptop saya sebelum	$.880^{**}$ .000	Valid
[B18] Ketika Pearson hasil cetakan Correla dokumen tion rahasia perlu Sig. (2- dibuang, saya tailed) memastikan bahwa itu robek N atau	$.883^{**}$ .000	Valid
[B19] Saya Pearson tidak akan Correla mencolokkan tion USB Flash Sig. (2- Drive yang tailed) ditemukan di tempat umum ke N	$.841^{**}$ .000	Valid
[B20] Jika Pearson saya melihat Correla seseorang tion bertingkah Sig. (2- mencurigaka tailed) n di tempat kerja, saya	$.762^{**}$ .000	Valid
[B21] Jika Pearson saya melihat Correla insiden tion keamanan, Sig. (2- saya akan tailed) melaporkann N	$.883^{**}$	Valid

Based on Table 8, all variables have passed the specified cut-off value (> 0.8). This means that all variables have excellent reliability.

Table 14. Reliability each variable

Variable	*Cronbach's Alpha*	Sum of Item
Knowledge (K)	0.874	21
Attitude (A)	0.906	21
Behaviour (B)	0.913	21
All (K,A,B)	0.962	63

D. Information Security Awareness Level

The purpose of this study is to measure the level of information security awareness in MSMEs. The number of questions was 63 items with six answer options in the form of a Likert scale. If each respondent answers each question on a scale of 6, the total scale for all questions is 6426.

Table 15. Sum of scale each variable

Knowledge	Attitude	Behavior	Total
1659	1785	1797	5241

So to get the level of awareness from MSMEs are:

$$\left(\frac{5241}{6426}\right) \times 100\% = 81{,}56\%$$

Based on Table 2, the level of information security awareness is at the GOOD stage. However, this result cannot be generalized because the number of respondents did not meet the target to generalize the results.

4. Discussion

This research has flaws in terms of aspects of data collection, namely the number of respondents, only 17 of the 384 respondents needed. However, based on data processing done, such as validity, reliability, and normality in general, get good results.

When testing the validity, only a few variables are invalid, such as K15, K17, K9, K13, K1, K2, A12, A1, A2, B2, B3, B4, and B14. Overall valid variable items are 79.4%. In contrast, the reliability of each variable K, A, and B is reliable. Nevertheless, for the data normality test, only the Attitude (A) variable has not been typical.

5. Recommendations

Based on research data, recommendations are focused on passwords, internet access, file sharing, and e-mail. This is because respondents experienced severe problems with this. The use of passwords should be limited to social media and activities. The password is one of the benchmarks; if we neglect to pay attention to it will be fatal. It is recommended that recommendations from each application, for example, use a combination of letters, numbers, and symbols.

If the use of the internet is one of the main activities, we should ensure that every website, we visit is safe from viruses or malware. We recommend that we use an antivirus that always updates virus definition, especially those that can prevent viruses or malware from interacting on the internet. If we are in the public room, for example, café, wi-fi areas and so on, we should make sure the environment is safe. However, if we do not know that the environment is safe, but we are forced to work there, it would be nice to use a VPN (Virtual Private Network). The use of a VPN minimizes the occurrence of hacker attacks, but the use of antivirus must always be ensured always to update the virus definition.

Phishing threatens email users, especially businesspeople. Therefore, some things that need to be known to avoid these phishing attacks are alert. Make sure we do not open any incoming e-mail, especially e-mails and e- mail attachments. If the email is sourced from a client or a customer, we should first confirm with the client.

6. Conclusions

Information security awareness is critical in the current era of information technology. Every IT actor must always evaluate information security awareness. Vigilance is the key to preventing the emergence of information security threats.

This study evaluates MSMEs in Indonesia but is constrained by the number of MSMEs participating. There were 384 MSMEs needed, but only 17 were collected—data processing using these data resulted in a reasonably good test on reliability, validity, and normality. When assessing the validity, only a few variables are invalid, such as K15, K17, K9, K13, K1, K2, A12, A1, A2, B2, B3, B4, and B14. Overall valid variable items are 79.4%. In comparison, the reliability of each variable K, A, and B is dependable. However, for the data normality test, only the Attitude (A) variable has not been standard. The development of this research is very much expected, especially from data collection, because this study was only able to get 17 respondents.

Acknowledgement

The authors express their sincere gratitude to the Centre for General Studies and Co-curricular, Universiti Tun Hussein Onn Malaysia (UTHM) for its support.

References

[1] Aghakhani, N., Kalantar, H., & Salehan, M. (2016). Adoption of Implicit eWOM in Facebook: An Affect-as-Information Theory Perspective.

[2] Ahmad, N., Mokhtar, U. A., Fariza Paizi Fauzi, W., Othman, Z. A., Hakim Yeop, Y., & Huda Sheikh Abdullah, S. N. (2019). Cyber Security Situational Awareness among Parents. Proceedings of the 2018 Cyber Resilience Conference, CRC 2018. https://doi.org/10.1109/CR.2018.8626830

[3] Akraman, R., Candiwan, C., & Priyadi, Y. (2018). Pengukuran Kesadaran Keamanan Informasi Dan Privasi Pada Pengguna Smartphone Android Di Indonesia. JURNAL SISTEM INFORMASI BISNIS, 8(2), 115. https://doi.org/10.21456/vol8iss2pp115-122.

[4] Almadhoun, N. M., Dominic, P. D. D., & Woon, F. L. (2011). Perceived Security, Privacy, and Trust concerns within Social Networking Sites. IEEE International Conference on Control System, Computing and Engineering, 426–431. https://doi.org/10.1109/ICCSCE.2011.6190564

[5] Alotaibi, F., Furnell, S., Stengel, I., & Papadaki, M. (2017). A survey of cyber-security awareness in Saudi Arabia. 2016 11th International Conference for Internet Technology and Secured Transactions, ICITST 2016, 154–158. https://doi.org/10.1109/ICITST.2016.7856687

[6] Amin, M. (2014). PENGUKURAN TINGKAT KESADARAN KEAMANAN INFORMASI MENGGUNAKAN MULTIPLE CRITERIA DECISION ANALYSIS (MCDA) INFORMATION SECURITY AWARENESS LEVEL MEASUREMENT USING MULTIPLE CRITERIA DECISION ANALYSIS (MCDA). Jurnal Penelitian Dan Pengembangan Komunikasi Dan Informatika Vol, 5(1).

[7] Apip, M. (2018). Pajak UMKM Setengah Persen, Kado Lebaran Terindah. Retrieved July 27, 2019, from https://www.pajak.go.id/id/artikel/pajak- umkm-setengah-persen-kado-lebaran-terindah

[8] Ayuwuragil, K. (2017). Kemenkop UKM: 3,79 Juta UMKM Sudah Go Online. Retrieved September 12, 2019, from https://www.cnnindonesia.com/ekonomi/20 171115161037-78-255819/kemenkop-ukm-379-juta-umkm-sudah-go-online

[9] Bada, M., & Nurse, J. R. C. (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

[10] Bibi, A., Hussain, Z., Khan, F., & Maqsood, A. (2017). Quantitative evaluation of Security and Privacy perceptions in online social networks: A case study. 2017 14th International Bhurban Conference on Applied Sciences and Technology (IBCAST), 425–433. https://doi.org/10.1109/IBCAST.2017.7868089

[11] Budi, D. S., & Tarigan, A. (2018). KONSEP DAN STRATEGI EVALUASI MANAJEMEN KEAMANAN INFORMASI MENGGUNAKAN INDEKS KEAMANAN INFORMASI (KAMI) DAN EVALUASI KESADARAN KEAMANAN INFORMASI PADA PENGGUNA. METIK JURNAL, 2(1), 53–64

[12] Bühler, J., Murawski, M., & Bick, M. (2017). Should We Disable the Comment Function on Social Media? The Impact of Negative eWOM on Consumers' Trust in Fashion Presentations. https://doi.org/10.1007/978-3-319-68557-1_29

[13] Chu, S. C., & Sung, Y. (2015). Using a consumer socialization framework to understand electronic word-of-mouth (eWOM) group membership among brand followers on Twitter. Electronic Commerce Research and Applications, 14(4), 251–260. https://doi.org/10.1016/j.elerap.2015.04.002

[14] Danniswara, R., Sandhyaduhita, P., & Munajat, Q. (2017). The Impact of EWOM Referral, Celebrity Endorsement, and Information Quality on Purchase Decision. Information Resources Management Journal, 30(2), 23–43. https://doi.org/10.4018/IRMJ.2017040102

[15] Destya, S. (2018). MODEL PENGUKURAN TINGKAT KESADARAN KEAMANAN INFORMASI DI UNIVERSITAS AMIKOM YOGYAKARTA. SEMNASTEKNOMEDIA ONLINE, 6(1), 1–12.

[16] Direktorat Jenderal Pembelajaran dan Kemahasiswaan. (2019). Hari UMKM Internasional. Retrieved July 27, 2019, from https://belmawa.ristekdikti.go.id/2019/06/21/hari-umkm-internasional/

[17] Erkan, I., & Evans, C. (2016). The influence of eWOM in social media on consumers' purchase intentions: An extended approach to information adoption. Computers in Human Behavior, 61, 47–55. https://doi.org/10.1016/j.chb.2016.03.003

[18] Foltz, C. B., Newkirk, H. E., & Schwager, P. H. (2016). An Empirical Investigation of Factors that Influence Individual Behavior toward Changing Social Networking Security Settings. Journal of Theoretical and Applied Electronic Commerce Research, 11(2), 1–15.

[19] Gkioulos, V., Wangen, G., Katsikas, S., Kavallieratos, G., & Kotzanikolaou, P. (2017). Security Awareness of the Digital Natives. Information, 8(2), 42. https://doi.org/10.3390/info8020042

[20] Gupta, T., Choudhary, G., & Sharma, V. (2018). A Survey on the Security of Pervasive Online Social Networks (POSNs). Journal of Internet Services and Information Security (JISIS), 8(2), 48–86

[21] Gvili, Y., & Levy, S. (2018). Consumer engagement with eWOM on social media: the role of social capital. Online Information Review, 42(4), 482–505. https://doi.org/10.1108/OIR-05-2017-0158

[22] Hsu, L.-C., Chih, W.-H., & Liou, D.-K. (2016). Investigating community members' eWOM effects in Facebook fan page. Industrial Management & Data Systems, 116(5), 978–1004. https://doi.org/10.1108/IMDS-07-2015-0313

[23] Islami, D. C., IH, K. B., & Candiwan, C. (2016). Kesadaran Keamanan Informasi pada Pegawai Bank x di Bandung Indonesia. INKOM Journal, 10(1), 19–26

[24] Jumiati, Indarjani, S., & Sofiana, D. D. (2011).Pembinaan Kesadaran Keamanan Informasi di Lingkungan Sekolah Tinggi Sandi Negara Berdasarkan National Institute of Standard and Technology (NIST). E-Indonesia Initiative Forum 7th (EII2011), 1–7.

[25] Kabanda, S., Tanner, M., Kent, C., Kabanda, S., Tanner, M., & Kent, C. (2018). Exploring SME cybersecurity practices in developing countries Exploring SME cybersecurity practices

in developing countries. Journal of Organizational Computing and Electronic Commerce, 28(3), 269–282. https://doi.org/10.1080/10919392.2018.1484598

[26] Kapoor, P. S., Jayasimha, K. R., Gunta, S., & Sadh, A. (2019). Facebook eWOM. International Journal of Online Marketing, 9(3), 23–48. https://doi.org/10.4018/IJOM.2019070102

[27] Kasl, F. (2018). CYBERSECURITY OF SMALL AND MEDIUM ENTERPRISES IN THE ERA OF INTERNET OF THINGS. The Lawyer Quarterly, 28(2), 165–188.

[28] Kaušpadienė, L., & Ramanauskaitė, S. (2019). INFORMATION SECURITY MANAGEMENT FRAMEWORK SUITABILITY ESTIMATION FOR SMALL AND MEDIUM ENTERPRISE. 25(5), 979–997.

[29] Kominfo. (2017). UMKM Go Online, Upaya Wujudkan Visi "Digital Energy of Asia." Retrieved July 27, 2019, from https://www.kominfo.go.id/content/detail/9514/umkm-go-online-upaya-wujudkan-visi- digital-energy-of-asia/0/berita_satker

[30] Kompas. (2016). UMKM Sukses Mengurangi Pengangguran. Retrieved from https://republika.co.id/berita/koran/ekonomi-koran/16/11/22/oh1a8b4-umkm-sukses-mengurangi-pengangguran

[31] Kompas. (2017). UMKM Jadi Sektor Strategis untuk Perangi Kemiskinan. Retrieved July 27, 2019, from https://ekonomi.kompas.com/read/2017/09/16/081500826/umkm-jadi-sektor-strategis-untuk-perangi-kemiskinan

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

[33] Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. Computers & Security, 25(4), 289–296. https://doi.org/10.1016/j.cose.2006.02.008

[34] Lejaka, T. K., Da Veiga, A., & Loock, M. (2019). Cyber security awareness for small, medium and micro enterprises (SMMEs) in South Africa. 2019 Conference on Information Communications Technology and Society (ICTAS), 1–6.

[35] Lopes, I. M., & Pereira, J. P. (2017). Information Security in Virtual Social Networks: A Survey in Higher Education. WorldCIST 2017: Recent Advances in Information Systems and Technologies, 570, 774–782. https://doi.org/10.1007/978-3-319-56541-5

[36] Maulidha, H. (2018). Pengaruh kepribadian hexaco, pengalaman training, dan jenis kelamin terhadap kesadaran keamanan informasi di Dunia Maya. Fakultas Psikologi UIN Syarif Hidayatullah Jakarta.

[37] Menard, P., & Sharma, S. (2017). Competitiveness on Social Networking Sites and Its Implications on Individuals ' Security and Privacy Concerns. 50th Hawaii International Conference on System Sciences, 4928–4936.

[38] Merdeka. (2018). UMKM Sumbang 60 Persen ke Pertumbuhan Ekonomi Nasional. Retrieved July 27, 2019, from https://www.liputan6.com/bisnis/read/3581067/umkm-sumbang-60-persen-ke- pertumbuhan-ekonomi-nasional

[39] Natasia, Y. (2018). Evaluasi kesadaran keamanan informasi pegawai: Studi kasus otoritas jasa keuangan= Evaluation of employee's information security awareness: Case study Financial services authority of Indonesia. Universitas Indonesia. Fakultas Ilmu Komputer.

[40] Palos-Sanchez, P., Saura, J. R., & Martin-Velicia, F. (2019). A study of the effects of programmatic advertising on users' concerns about privacy overtime. Journal of Business Research, 96(October 2018), 61–72. https://doi.org/10.1016/j.jbusres.2018.10.059

[41] Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. Computers & Security, 66, 40–51. https://doi.org/10.1016/j.cose.2017.01.004

[42] Puspitaningrum, E. A., Devani, F. T., Putri, V. Q., Hidayanto, A. N., Solikin, & Hapsari, I. C. (2018). Measurement of Employee Information Security Awareness: Case Study at A Government Institution. 2018 Third International Conference on Informatics and Computing (ICIC), 1–6. https://doi.org/10.1109/IAC.2018.8780571

[43] Sekaran, U., & Bougie, R. (2016). Research methods for business: A skill building approach. John Wiley & Sons.

[44] Sohaib, M., Hui, P., Akram, U., Majeed, A., Akram, Z., & Bilal, M. (2019). Understanding the Justice Fairness Effects on eWOM Communication in Social Media Environment. International Journal of Enterprise Information Systems, 15(1), 69–84. https://doi.org/10.4018/IJEIS.2019010104

[45] Sriratanaviriyakul, N., Nkhoma, M., Felipe, A. L., Cao, T. K., Tran, Q. H., Epworth, R., … Quang, H. Le. (2017). ASEAN users' privacy concerns and security in using online social networks. International Journal of Electronic Security and Digital Forensics, 9(1), 84. https://doi.org/10.1504/IJESDF.2017.081787

[46] Teng, S., Khong, K. W., Goh, W. W., & Chong, A.Y. L. (2014). Examining the antecedents of persuasive eWOM messages in social media. Online Information Review, 38(6), 746–768. https://doi.org/10.1108/OIR-04-2014-0089

[47] Tran, T. P. (2017). Personalized ads on Facebook: An effective marketing tool for online marketers. Journal of Retailing and Consumer Services, 39(March), 230–242.

[48] ULTA, R. O. (2018). ANALISA PERILAKU PENGGUNA SMARTPHONE BERDASARKAN INFORMATION SECURITY AWARENESS THEORY TERHADAP KEAMANAN INFORMASI. Universitas Islam Negeri Sultan Syarif Kasim Riau.

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

[50] Wang, J. J., Wang, L. Y., & Wang, M. M. (2018). Understanding the effects of eWOM social ties on purchase intentions: A moderated mediation investigation. Electronic Commerce Research and Applications, 28, 54–62. https://doi.org/10.1016/j.elerap.2018.01.011

[51] Wu, L.-L., Wang, Y.-T., & Hsu, A.-C. (2014). Ewom effects on Facebook. PACIS, 95.

[52] Yan, Q., Wu, S., Zhou, Y., & Zhang, L. (2018). How differences in eWOM platforms impact consumers' perceptions and decision- making. Journal of Organizational Computing and Electronic Commerce, 28(4), 315–333. https://doi.org/10.1080/10919392.2018.1517479

[53] Yan, Y. C., Li, H., & See-To, E. W. K. (2014). Fun In A Trustworthy Environment? The Effects of Message Source Credibility And Message Appeal On EWOM Responses In Facebook. UKAIS, 44.

[54] Yang, X. (2019). How perceived social distance and trust influence reciprocity expectations and eWOM sharing intention in social commerce. Industrial Management and Data Systems, 119(4), 867–880. https://doi.org/10.1108/IMDS-04-2018-0139

[55] Zeki, A. M., & Hamid, H. (2016). Evaluation of Users' Awareness and Their Reaction on Information Security. Proceedings - 2015 4th International Conference on Advanced Computer Science Applications and Technologies, ACSAT 2015, 251–255. https://doi.org/10.1109/ACSAT.2015.50