E-Commerce Internet Security among Women Entrepreneurs in East-Coast Malaysia.

Muhamad Saufi Che Rusuli[a], **Maslaini Mohamad Sapri**[b], **Noraani Mustapha**[c], **Suhaila Abdul Kadir**[d], **Anis Amira Ab Rahman**[e], **Josu Takala**[f], [a,b,c,d]Malaysian Graduate School of Entrepreneurship and Business, Universiti Malaysia Kelantan Kampus kota, 16100 Pengkalan Chepa Kelantan, [e]Faculty of Entrepreneurship & Business Universiti Malaysia Kelantan Kampus kota, 16100 Pengkalan Chepa Kelantan, [f]Faculty of Technology, University of Vaasa, Finland, Email: [a*]msaufi@umk.edu.my

This study aims to seek awareness of internet security especially among female entrepreneurs involved in e-commerce activities. Internet Security has its own significance in every aspect of the industry. With the advance of internet technology (IT) and the ongoing modernization of electronic data networks, there has been a multi-dimension of doing business in Malaysia. This study was conducted using the qualitative approach and involved six respondents at every level of age from 25-30 years old, 31-35 years old and 36-40 years old. Thus, this study hopes to shed light on the current awareness of Internet security among women entrepreneurs especially in the East Coast region in Malaysia. Hence, the result from the study indicates that having the knowledge, understanding and experiences of e-commerce internet security is very crucial for every entrepreneur who was involved in online businesses.

Key words: *E-Commerce, Internet Security, Business, Sustainability, Online Business.*

Introduction

E-Commerce, a short form for “electronic commerce” is a process of conducting or processing business on the Internet. E-Commerce also known as e-business as their process and ways are very similar to each other. E-commerce holds a very important role in today’s business world. As the technologies evolve, the Internet is created and everything went online. This made people’s lives much easier as everything can be done by the tip of their fingers. There are many types of e-commerce such as online shopping, electronic payments, online auctions, internet banking and online ticketing. Online shopping is the most popular type of e-commerce (Fang, Chen, Wen, & Prybutok, 2018; Cano, Perry, Ashman, & Waite, 2017; Pirani, Marewar, Bhavnagarwala, & Kamble, 2017) where the activity of purchasing and selling goods on the Internet occurs. Customers will search and purchase their products of interest within single clicks of their mouse. For instance, amazon.com becomes the most famous online shopping destination. On the other hand, electronic payments are a mechanism of online payments, where when a buyer buys goods online, the payment processors and payment gateways will come into their minds (Razak & Pisal, 2016; Yusof, Abdullah, & Isa, 2016).

In every part of the world, especially a modern city such as Japan or United States, e-commerce is already advanced and sophisticated. However, in Malaysia, the level of knowledge among citizens about e-commerce is still moderate (Chong, Bian, & Zhang, 2016; Othman & Shahzad, 2016; Shaharuddin, Rahman, Aziz, & Kassim, 2018). On the east coast of Malaysia (e.g. Kelantan, Terengganu and Pahang), e-commerce is not really a big boom among the people as they prefer to do business face-to-face or hands-by-hands, although there are few sellers that already have established online business (e.g. boutiques, etc.). The question is how much knowledge and information do they have in order to sustain their online business and prevent online risks? When they put their business online, they are putting their own business at risk as well.

According to Lim San Peen, senior executive director at PwC Advisory services, Malaysia, stated that “in a world where most enterprises rely on technology, businesses are increasingly opening themselves up to the risk of criminal activity”(Yap, 2012). Also, in the 6th Global Economic Crime Survey conducted that was by PricewaterhouseCoopers (PwC), cybercrime is ranked as the top four economic crimes globally. Based on their findings, in Malaysia, only 5% of respondents were reported of being cybercrime victims while 28% respondents say they are likely to experience cybercrime perpetrated against their business and organizations. This shows that Malaysians awareness of cybercrimes and securing their online businesses is still in the level of learning. The government and authorities should empower the knowledge related to e-commerce security, cybercrimes and cyber security issues. Other than that, companies need to get a wide and comprehensive view of the entire IT risk landscape so they can manage the IT risks effectively. IT risks may evolve every time, but this holistic perspective will provide organizations with starting point to help them identify and manage current IT issues and challenges. Hence, there are several research objectives highlighted to be achieved as below:

i. To study the level of awareness regarding e-commerce Internet security of women entrepreneurs.

ii. To understand the importance of e-commerce Internet security in securing online business.
iii. To study the significance of securing online business by using e-commerce Internet security.

The awareness regarding e-commerce internet security among women entrepreneurs especially those resided on the east-coast of Malaysia is still unknown. Therefore, it is important to explore the level of knowledge regarding e-commerce internet security as it is a very crucial part for every online business.

Literature Reviews

Rising of Cybercrimes

According to senior executive director of PwC Advisory Services, Malaysia, stated that "In a world where most enterprises rely on technology, businesses are increasingly opening themselves up to the risk of criminal activity" (Yap, 2012). He also said that "Rising incidents of data loss and theft, computer viruses and hacking and other forms of electronic crime demonstrate the need of more cyber savvy approach to fraud prevention". Also, according to Ilias Chantoz, senior director of government affairs for Symantec Asia-Pacific, Japan and Europe, it is hard to determine whether Malaysia can cope or is aware of this issue because this is the first time they include Malaysia in their survey. So, in the survey regarding critical infrastructure protection (CIP) program by Cybersecurity Malaysia, 36% of the respondents are feeling neutral or do not have any opinion of matter to the CIP program. Other than that, 34% of the respondents feel like they were not engaged enough with the CIP program. So, in order to get a wide and perfect view of IT risk, organization must work on how effective they manage this issue.

E-commerce exists so the user can maximize their organization profit and customer services. But the level of internet security awareness among the community is never near to the expected one. However, there are organizations that found their way to secure their e-commerce networks. One of the organizations was Liberty Financial Cos. Inc. According to Hann (1999) in this organization matter, "To provide better security for their customers, Liberty uses digital certificates to verify the identity of the customer and the authenticity of the site. As a result of their efforts, 15 to 20 percent of brokers and customers conduct e-commerce with Liberty using digital certificates while other customers type in their names and passwords". In order to protect their data from damages, the anti-virus software needs to be updated every month.

Data Safety and Privacy

In e-commerce, the principal factor is trust. According to Adele et al (2001), on their research at South Africa, they stated that 50% of the respondents did not want to share their credit cards information while buying goods and services online although their online transaction was secure (Odiboh, Ben-Enukora, Oresanya, Yartey, & Aiyelabola, 2017). This was because they were concerned with the safety of their credit card information while transacting the business. They were also concerned that hackers might steal their card information. This shows the awareness of e-commerce security among the community was still low based on their studies, users with information technology knowledge tend to buy their things online because they have better knowledge and awareness on this issue.

Other than that, privacy is one of the factors that is included in the digital business arena. According to Technopedia, “internet privacy is the privacy and security level of personal data published via the Internet. It is a broad term that refers to a variety of factors, techniques and technologies used to protect sensitive and private data, communications and preferences”. Both sellers and consumers need to compromise their privacy while doing online transacting. Users might be unsure to do e-commerce because they did not know the extent their private information was made available for others to view.

Cultural Barriers

In Malaysia, the adoption of e-commerce into small and medium size enterprises (SMEs) is very difficult. One of the cultural barriers in e-commerce is the language of e-commerce. In order for sellers to attract more customers to buy their services and products, they need to be able to suppress the language of e-commerce. E-commerce is universal, so, customers with little knowledge of online business might not be able to understand the product’s description whether in English or other international languages. This will restrict the relationship between sellers and buyers. Government institutes in Malaysia should empower the Malaysians about the basic knowledge of e-commerce and how to buy online safely. This empowerment will be the future of Malaysia and improve their advantage such as evolving into a more developed country.

Awareness of E-commerce Internet Security Training

According to Microscope e-zine, “A cyber security awareness deficit amongst employees poses a major threat to UK organizations, according to a new study”. If an organization fails to give effective e-commerce security awareness and training to their employees, they will put their reputation, competitive advantage and customer trust at risk. Nick Wilding, head of cyber resilience best practice at Axelos mentioned that “despite organizations continuing to invest heavily in technology to better protect their precious information and systems, the number and scale of attacks continues to rise as they discover there is no ‘silver bullet’ to help them achieve their desired level of cyber security”. The awareness of e-commerce security training is a must in a business organization so that customers will feel at ease as their precious information is safe from any cyber related attack.

In Nigeria, the earlier studies of digital insecurity Adeniran (2008) stated that “the internet has not only facilitated the growth of internet crimes in Nigeria but has equally enhanced the level of sophistication of related finance-based criminality and modernization of criminality among the Nigerian youths” (Odiboh et al., 2017). If it is not properly controlled, it will cause more people to be victims of cybercrime. One of the security threats is phishing. According to Norton website by Symantec ("Online Fraud: Phishing,") “Phishing is essentially an online con game and phishers are nothing more than tech-savvy con artists and identity thieves. They use spam, fake websites, crime ware and other techniques to trick people into divulging sensitive information such as bank and credit card account details. Once they have captured enough victims’ information, they either use the stolen goods themselves to defraud the victims or they sell it on the black market for a profit”. In Nigeria, Phishing happened mostly on mobile users and is very harmful as most mobile applications and websites usually interact in ways that can be hacked.

In customer context, the awareness of e-commerce security for online customers in Malaysia is still a big issue. According to (Cagaoan et al., January 2014) “customer safety is a serious issue in electronic commerce, no matter what source on examines”. E-commerce is worldwide. So, the confidentiality of the data acquired must be kept securely against all types of threats.

Research method

This study is based on the interpretivist paradigm with realism ontology and conventionalism epistemological perspective. This study used qualitative method because it can reveal the complex issues’ phenomenon which is about the awareness of internet security among the technological user. Inductive strategy is employed for this study because the objective of this study is to understand the phenomenon through answering the research questions that contribute to solve the research problem. In line with that, this study selected relevant concepts and defined those concepts prior to the field investigation. The data sources for this study are observations, semi-structured interviews, impressions and reactions of researchers, documents and text. A non-probability sampling has been applied and six (6) participants have been selected based on the age level of 25-30 years old, 31-35 years old and 36-40 years old. The information from six participants is rigor enough since this study triangulated information from interviews with the other data sources as mentioned before. Furthermore, the information from interviews are in-depth enough since it took one and half hours of interview sessions and the indication of information saturation is emerged. The information from data sources are being analyzed using thematic analysis technique.

Discussion

The main objective of this study is to understand the awareness of E-Commerce Internet Security among women entrepreneurs in East-Coast Malaysia. It is found that women entrepreneurs' awareness level is promising. The findings indicate that women entrepreneurs understand the importance of e-commerce internet security in securing online business**.** Lastly, the finding reveals that women entrepreneurs understand the significance of securing online business by using e-commerce internet security. The discussion regarding the findings and objectives are as below:

Level of awareness regarding e-commerce internet security of women entrepreneurs

In general, it is found that women entrepreneurs are aware of e-commerce internet security and the younger generation has higher awareness level. Four of them have basic knowledge about e-commerce internet security, while the other two have no idea what e-commerce internet security is. The two respondents that have no knowledge of e-commerce internet security come from the ages 31-35 years old and 36-40 years old respectively. This shows that younger respondents; age level 25-30 years old, might have better knowledge and awareness regarding e-commerce internet security compared to the later respondents. The finding is in line with previous literature that indicates the young generation is more exposed to the computer and technology (Kang, Endacott, Gonzales, & Bengtson, 2019; Pradhan, Panda & Prasad, 2018).

The awareness level is existing since the women entrepreneurs have taken some measures to secure their online business such as changing the passwords and not sharing their bank account number publicly and also think that their online businesses are secured enough. Although the awareness level of women entrepreneurs exist, they should enhance their knowledge on e-commerce internet security. The factor that contributes to the low level of awareness may draw from the feeling of safety because they haven't experienced online fraudulent activities in their online business. This situation is confirmed by the previous research finding that indicates people that never experienced any fraudulent activities in their online business might lower their guard down regarding the security of their online business (Adamkolo, Hassan & Pate, 2018). The awareness of e-commerce internet security through knowledge inculcation can be done easily since the women entrepreneurs indicated that e-commerce internet security is easy to be applied to their online businesses.

Lastly, the women entrepreneurs believe that their investment on internet security will improve their business. This belief is due to the safe guard of their data, the trust that customers feel because they feel safe doing online transaction that can secure them from fraudulent activities. Previous studies have indicated that feeling of safe and trust contribute to the investment decision (Agag, 2019; Khan, Akter & Zeya, 2019; Smith-Ditizio & Smith, 2019).

The importance of e-commerce internet security in securing online business

This study found that, women entrepreneurs understand the importance of e-commerce Internet security in securing online business. In modern e-commerce businesses, the importance of e-commerce internet security cannot be over exaggerated. Personal information of people all around the globe are exposed only with a tiny security oversight. In e-commerce, the most important data for both sellers and customers are their bank accounts' numbers, passwords to access to their business page and any other personal information that matters. So, the importance of e-commerce internet security in securing online business is very crucial.

Those women entrepreneurs understand that the element of trust is very important in e-commerce internet security. Customers see this as one of the key factors when they want to do online business. Women entrepreneurs inform that by implementing e-commerce internet security, the online business will increase the level of trust among customers and sellers themselves. Customers will feel very secure to do transactions in their online business because they knew that their data and integrity were protected. For example, by installing a SSL certificate to the online business, it will inform the customers that their transactions are well encrypted. The padlock in the address bar of the business page also indicates that the page is secure and the customers will have faith doing business with them.

The women entrepreneurs also understand the importance of e-commerce internet security in securing online business is it can prevent any cyber threats from attacking the business page and stealing personal information. Cyber threats can be classified into several types such as malware, ransomware, distributed denial of service (DDoS) attacks, phishing, corporate account takeover (CATO) and automated teller machine (Bakti & Sumaedi) cash out. The most common threats that threat any e-commerce business are malware, phishing and corporate takeover (CATO).

According to Mass.gov website, malware is known as "malicious code or malicious software program inserted into a system to compromise the confidentiality, integrity or availability of data". They also stated that "malware has become one of the most significant external threats to systems and can cause widespread damage and disruption, as well as requires huge efforts within most organizations".

Also, according to Mass.gov website, phishing is "a form of social engineering, including attempts to get sensitive information and the attempts will appear to be from a trustworthy person or business". An example of phishing activities include fake websites or email address that looked exactly like an original one. Last but not least, corporate account takeover (CATO). According to Mass.gov website, CATO is "a business entity theft where cyber thieves impersonate the business and send unauthorized wire and ACH transactions. The unauthorized funds are sent to accounts controlled by the cybercriminal".

Most of e-commerce businesses are exposed and vulnerable to all of the threats mentioned. Online businesses with low e-commerce internet security are easy targets for the cybercriminals. This is why e-commerce internet security is very important to secure online businesses so that they will not be exposed and targeted by the cybercriminals.

The significance of securing online business by using e-commerce internet security

It is found that the women entrepreneurs understand the meaning and significance that can be described as the quality of being worthy of attention which relates to securing online business. The quality of some of e-commerce internet security platforms must be ensured in order to have a good security for online businesses. According to Maurer (2017), there are four qualities of an outstanding e-commerce internet security platform.

First is that, the e-commerce internet security platform must be adjusted to the applicants budget. If the seller has just started his/her online business, they probably do not want to spend so much on setting an e-commerce internet security for the business page. So, a good e-commerce internet security platform must be adjusted to the sellers' budget no matter how small their business is. As in every e-commerce business created, there will be data and personal information to be protected.

Second is, the e-commerce internet security platform must keep the data secure. It is a priority for every online seller to protect their customers' information and confidentiality. If the sellers used an unsecured e-commerce internet security platform, this will cause catastrophic events such as data theft. Therefore, there will be a breach of trust between sellers and their customers. So, having a good quality e-commerce internet security platform is a must for every online business.

Third, the e-commerce internet security platform must also be fast. Fast is in the context of how quick it loads and the amount of time needed for the platform to detect any malware and malicious activities in the businesses site. Thus, a quality e-commerce internet security platform must be fast in order to secure the online businesses.

Fourthly, a quality e-commerce internet security platform must be easy to use for both customers and sellers. Sometimes, a complicated e-commerce internet security platform will take a longer time to run and will create so much fuss that some of the online sellers prefer to not to take any security measures for their business at all. A good quality e-commerce internet security platform should not require the users to spend a lot of time trying to figure out how to use it accordingly. So, the easier e-commerce internet security applied, the better the platform itself.

So, it is very significant to use a good quality of e-commerce internet security platform in order to secure the online business. This will increase the significance for both customers and sellers.

Conclusion

In summary, this study is about the awareness of technological security among the women entrepreneur as technological user. It reveals that the women entrepreneurs on the East-Coast of Malaysia are aware of E-Commerce Internet Security. This study also indicates that having the knowledge of e-commerce internet security is very crucial for everyone who has online businesses. It is because e-commerce internet security holds great function in securing online businesses and it should become one of the main tools in every online business. The motive of applying e-commerce internet security to their online business are to increase the security of their online business pages, securing the online transaction, increase the trust of customers towards their business, made their work easier and others. It is clearly showed that the usage of e-commerce internet security as one technology platform gives more advantages for both online sellers and customers. Besides that, the business activities are more efficient and safer from cyber threats with the support of e-commerce internet security. Therefore, it is better for future research to collect as much data as possible regarding e-commerce internet security without being bound to any location or area.

REFERENCES

Adamkolo, M., Hassan, M., & Pate, A. (2018). Consumers' Demographic Factors Influencing Perceived Service Quality in e-Shopping: Some Evidence from Nigerian Online Shopping. *Pertanika Journal of Social Sciences & Humanities, 26*(3), 1335-1369

Agag, G. (2019). E-commerce Ethics and Its Impact on Buyer Repurchase Intentions and Loyalty: An Empirical Study of Small and Medium Egyptian Businesses. *Journal of Business Ethics, 154*(2), 389-410.

Bakti, I. G. M. Y., & Sumaedi, S. (2013). An analysis of library customer loyalty: The role of service quality and customer satisfaction, a case study in Indonesia. *Library Management, 34*(6/7), 397-414.

Cagaoan, A, A. K., Buenaobra, M.J.V., A., Martin, Trina, . . . Jonathan. (January 2014). Privacy Awareness in E-commerce. *International Journal of Education and Research, 2*(1).

Chong, W. K., Bian, D., & Zhang, N. (2016). E-marketing services and e-marketing performance: the roles of innovation, knowledge complexity and environmental turbulence in influencing the relationship. *Journal of Marketing Management, 32*(1-2), 149-178.

Fang, J., Chen, L., Wen, C., & Prybutok, V. R. (2018). Co-viewing Experience in Video Websites: The Effect of Social Presence on E-Loyalty. *International Journal of Electronic Commerce, 22*(3), 446-476.

Kang, S. L., Endacott, C. G., Gonzales, G. G., & Bengtson, V. L. (2019). Capitalizing and Compensating: Older Adults’ Religious and Spiritual Uses of Technology. *Anthropology & Aging, 40*(1), 14-31.

Khan, S. N., Akter, M., & Zeya, F. (2019). Bangladeshi Banking Innovations: A Case Study on Mobile Banking *Business and Management Practices in South Asia* (pp. 101-124): Springer.

Odiboh, O., Ben-Enukora, C., Oresanya, T., Yartey, D., & Aiyelabola, A. (2017). Awareness on Digital Security and E-business in Nigeria. 7.

Online Fraud: Phishing.   Retrieved from https://us.norton.com/cybercrime-phishing

Othman, S., & Shahzad, A. (2016). The Mediating Effects of Behavioural Intention of the Acceptance and Use of E-Commerce among SMEs in Kedah, Malaysia. *Science International, 28*(3), 3173 -3178.

Pirani, Z., Marewar, A., Bhavnagarwala, Z., & Kamble, M. (2017). *Analysis and optimization of online sales of products.* Paper presented at the Innovations in Information, Embedded and Communication Systems (ICIIECS), 2017 International Conference on.

Pradhan, K., Panda, S., & Prasad, C. V. (2018). Perceiving The Behavioral Change of Farmers Through Modern Information Communication Technology (ICT) Tools. *Indian Research Journal of Extension Education, 18*(2), 46-53.

Razak, N. A., & Pisal, F. N. A. (2016). Development of Muslim Women Social Entrepreneurs: Towards Digital Economy. *International Journal of Business, Economics and Law, 9*(5), 52-57.

Shaharuddin, N. A., Rahman, A. A., Aziz, Y. A., & Kassim, S. (2018). An Assessment of Web Technologies & E-Business Adoption Among Smes Travel Agencies in Malaysia. *Journal of Academia UiTM Negeri Sembilan Vol, 6*(1), 89-96.

Smith-Ditizio, A. A., & Smith, A. D. (2019). Computer Fraud Challenges and Its Legal Implications *Advanced Methodologies and Technologies in System Security, Information Privacy, and Forensics* (pp. 152-165): IGI Global.

Yap, E. (2012, January 2, 2012). Awareness of Cyber Security Still Lacking. *The Edge Malaysia*.

Yusof, R., Abdullah, N., & Isa, F. M. (2016). *Impact Of E-Business Applications For Business Success Among Malay Women Entrepreneurs*. Paper presented at the 2nd International Conference on ASEAN Women.