# CULTURAL COMPARISON TOWARDS USERS' SUSCEPTIBLE TO PHISHING EMAILS

**Ibrahim Mohammed Alseadoon [1] and Mohd Fairuz Iskandar Othman [2],**

[1]University of Ha'il, Hail, Saudi Arabia, [2]Universiti Teknikal Malaysia Melaka, Malaysia

**Abstract**

Phishing emails are causing enormous financial losses for both businesses and individuals. One key element that increases phishing emails success is users. Understanding users who become victims to phishing emails will help in reducing success rate. Our study uses quantitative approach in attempt to understand key factors that affecting users' vulnerability to phishing emails. Identified factors are compared across cultures mainly: Malaysian, Australia, and Saudi Arabian cultures. The main goal of our study is to find culture impact on users' vulnerability. Our results indicate that users' vulnerability to phishing emails is different across cultures. It can be said that there are factors that have the opposite impact in different cultures, while other factors have the same impact despite culture differences.

***Key words:***

*Security, Phishing, email, behaviour, users.*

## 1. Introduction

Phishing emails do not distinguish between local and international organisations or individuals. Their target is any entity that has connection to the Internet. Therefore, the threats of phishing emails are massive. The financial losses caused by phishing emails are enormous worldwide [1]. This problem did not go unnoticed. Many researchers have tried to resolve and eliminate phishing emails damages finically and psychology [2]. Nowadays, phishing emails are being used to launch cyber wars between countries [3]. Majority of phishing emails have one main objective which is luring users to perform a certain action. The results of that action will harm users directly or indirectly. Therefore, fighting these types of emails became a necessity for many organisations.

Different defences have been introduced in many forms. The first defence to phishing emails is to identify them automatically and remove them before they encountered with users [4, 5]. This defence has helped in stopping emails from reaching users. Some of the solutions have reached around 90 percent correct identification for phishing emails. However, there are still 10 percent of phishing emails reaching users. Phishing emails have the danger that one phishing email can result in high damages for users and organisations. Therefore, users were included in the defence solutions in attempt to stop them from responding to phishing emails.

These solutions started by understanding why users fall victims to phishing emails [6, 7]. Afterwards, educational materials were introduced to help users not to respond to phishing emails [8-10]. Some defences introduced a combination between technical solutions and awareness solutions such as new bar colour or symbols in explorers such as padlock. However, there are still users who still become victims to phishing emails. Additionally, most of phishing emails studies are limited to one type of users group. Our study is trying to fill this gap by understanding the nature of users and their group differences which make them fall victims to phishing emails by studying users from difference cultures.

## 2. Culture differences

Culture differences can be identified using Cultural Dimension Theory developed by Hofstede [7]. Hofstede distinguished Cultures based on five main dimensions that are: Power Distance Index (PDI), Individualism vs. collectivism (IDV), Uncertainty Avoidance (UAI), Masculinity vs. femininity (MAS), Long-Term Orientation vs. short-term orientation (LTO), and Indulgence vs. restraint (IND).

Based on Hofstede Cultural Dimension Theory, our study chose Malaysian, Australian, and Saudi Arabian cultures as the main cultures for investigation. The reason for choosing these three cultures is: (1) the authors of this study know these cultures. (2) Questionnaire distribution and data collection can be monitored easily by researchers. (3) Results analysis and recommendations will be supervised for implementation. (4) Both authors lived in these cultures and experience its implications. Table 1 gives details about the degree of each dimension based on Cultural Dimension Theory.

Manuscript received October 5, 2021
Manuscript revised October 20, 2021
https://doi.org/10.22937/IJCSNS.2021.21.10.33

**Table 1:** Cultural Dimension Results

| | **Malaysia [8]** | **Saudi Arabia [9]** | **Diff.** | **Australia [10]** | **Diff.** |
|---|---|---|---|---|---|
| PDI | 100 | 95 | 5 | 38 | 62 |
| IDV | 26 | 25 | 1 | 90 | -64 |
| UAI | 36 | 80 | -44 | 51 | -15 |
| MAS | 50 | 60 | -10 | 61 | -11 |
| LTO | 41 | 36 | -5 | 21 | 20 |
| IND | 57 | 52 | 5 | 71 | -14 |

Form Table 1, there are differences between Malaysian culture, Saudi Arabian culture, and Australian culture. In Saudi Arabian culture, the dimensions: UAI, MAS, and LTO have higher scores than Malaysian dimensions. Dimensions: PDI, IDV, and IND have lower scores in Saudi Arabia and the variances are low. While in Australia, the dimensions: IDV, UAI, MAS, and IND have higher scores and the variances are high. Dimensions: PDI and LOT have lower scores in Australian dimensions and the variances are also high. In summary, Australian Dimensions have higher variances than Malaysian ones. While in Saudi Arabian dimensions the variances are not high except some dimensions. Despite that, it can be seen there are variances between Saudi Arabian and Malaysian Dimensions.

## 3. Methodology

Our study is based on a quantitative method approach. An online questionnaire was developed based on [3] study. The questionnaire was distributed using an online survey administration application namely Google forms [6].The responses were recorded using the same application. The questionnaire targeted Malaysian users to compare their results with previous obtained results from Australian and Saudi Arabian users [3]. The main aim of the study is to measure the impact of cultural differences on users' likelihood to respond to phishing emails.

The questionnaire was presented to bachelor students from both genders. The design of the questionnaire is to collect demographic information about the participants as well as five latent variables. Additionally, the questionnaire included 38 items about potential factors affecting users' susceptibility to phishing emails. The dependent factor in our study is users' likelihood to respond to phishing emails. Participants were presented with 4 phishing emails and 2 legitimate emails. Participants were asked to rate their likelihood to respond to these emails using 5-point Likert scale [11]. The dependent latent variables are Trust, Submissiveness, Internet activities, Perceived email experience and richness. 213 participants fully answered the questionnaire. The results are explained in the following section.

## 4. Analysis and results

We used factor analysis to analyse collected data using SPSS software. Additionally, SEM modelling was used to validate the proposed model using SmartPLS software. The results of the analysis are explained below.

### 4.1 Demographic differences

Four main demographic differences were measured namely: age, gender, language, and nationality. Age group at the beginning were divided into three groups as used in the previous study [3]. Furthermore, due to lesser number of participants in age group 3 (36 and above), group 3 was merged with group 2 to become (26 and above). Therefore, a t-test was used to measure age groups variance: 18 to 25 (group 1) and 26 and above (group 2). The results show that there is a significant difference between the two groups (p value < 0.001). Younger users are more likely to respond to phishing emails than older users.

The three demographic variables results are as follows: (1) regarding gender differences, there are no significant differences between male and female likelihood to respond to phishing emails. (2) Regarding language differences, there are no significant differences between users who their first language is different than others. (3) Regarding nationality differences, there are no significant differences between users who have different nationality than other users.

### 4.2 Latent variables

The results of the five latent variables are as follows. All three items for trust factor are loaded together [12]. Submissiveness factor included 6 items 1 – 5 and 8 are used to measure submissiveness [1]. The rest of the items show less load on the latent variable. Internet activities have been measured with three items which are: reading, communication, and shopping and the three items loaded together. Email experience was measured with 6 items [4]. Five of them loaded together for the latent variable. Email richness was measured with 4 items [4]. All four items loaded together. Likelihood to respond to phishing emails were measured by 6 items. 4 items were loaded together. Two items were excluded that are phishing emails 2 and legitimate email 2. These two items did not fit the cut-off criteria to be included in the latent variable.

### 4.3 Analysis based on SmartPLS software

SEM modelling was used in our analysis to measure latent variables impact. The results are shown in Tables 2 and 3:

**Table 2**: Latent Variables Effect

| Variable | Effect | Path coefficient |
|---|---|---|
| Trust | Negative | 0.097 |
| Submissiveness | Positive | 0.275 |
| Internet usage | Positive | 0.132 |
| Email experience | Negative | 0.069 |
| Email richness | Positive | 0.288 |

**Table 3**: Model Fit

| | R-square |
|---|---|
| Likelihood to respond to phishing emails | 0.19 |

The results presented by our study explain around 20 percent of users' likelihood to respond to phishing emails (see Figure 1). Trust and perceived email experience have negative impact on making users less likely to respond to phishing emails. Submissiveness as expected have positive impact on making users more likely to respond to phishing emails. Surprisingly, Email richness has increased users' likelihood to respond to phishing emails. Internet activities have positive impact on making users more likely to respond to phishing emails.

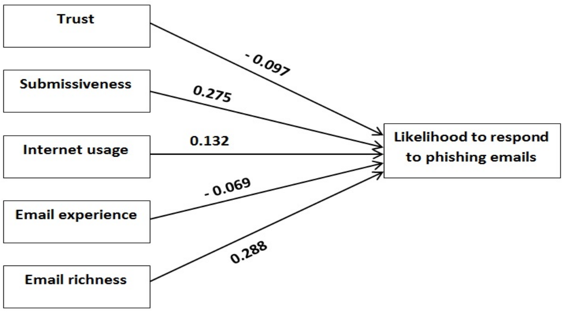

**Fig. 1:** Research model

## 5. Discussion

Regarding demographic differences, there are differences between Malaysian, Australian, and Saudi Arabian users. Our studies show that age has a significant impact between users. Younger users are more willing to respond to phishing emails. It can be said that younger users are more towards risk taking than older users. Also, it can be the nature of younger users who are more willing to not making rational decisions as phishing emails deceive users. Gender has no significant differences between our studies. In Australian study, Nationality shows significant impact on users' vulnerability where Malaysian study did not show any significant differences. Nationality differences can be related to dimension IDV as Australian users have high score which relate to users take responsibility on individual rather than groups. Therefore, group differences can be seen. Finally, language, there were no significant differences in Malaysian study where Australian study, shows that language does impact users' likelihood to respond. One observation of language finding is that phishing emails used in our study were presented in English language as it is among the main language of use in Malaysia. It can be said that the results may differ if the main language used for phishing emails was Bahasa Malaysia, which is the national language.

### 5.1 Differences

Surprisingly, three variables behaved differently than expected: trust, email richness, and Internet activities. Unlike in the Australian study, trust has negative impact on making users less likely to respond to phishing emails. It was expected that trust will increase users' likelihood to respond. Especially that Trust makes users more willing to give their trust even in situations of doubt. However, the results suggest the opposite. One explanation can be found in the dimension UAI, where Malaysian users score higher than Australian users, which relates to control uncertain situation. Therefore, Malaysian users might doubt the phishing emails but choose not to respond till they have a certain confirmation that responding to the email is safe. Even though, Malaysian users are more willing to give trust. However, this trust will not be translated to action in doubt situation.

Email richness was expected to make users less likely to respond to phishing emails. Especially that Australian study shows that email richness reduced users' likelihood to respond to phishing emails while Saudi Arabian study did not show any significance. However, our study shows that email richness has increased Malaysian users' likelihood to respond to phishing emails. Email richness means that users are able to gain rich information from an email [4]. Email as a medium is considered as a poor medium which cannot include rich information such as person to person conversation [5]. However, recently new tools have been embedded in emails such as emojis which might have the impression that users can carry on more cues which results in considering emails as a rich medium. Considering emails as a rich medium, made Malaysian users more willing to respond to well-designed phishing emails. Additionally, the dimension MAS in Malaysian users is lower than Australian users, which relates to society performance for achievement. Therefore, Malaysian users used their perceived email richness to complete and perform requested tasks in phishing emails as a sense of achievement.

Internet activities have two effects. One of the effects agrees with previous studies while the other disagrees. In this section, we discuss the disagreement. Internet Activities were measured by three items: surfing, communicating, and shopping. It was expected that users who do more shopping on the Internet are more careful and able to recognise phishing emails. Shopping is very critical as it involves sending money over the Internet. Users who do shopping are expected to examine websites before giving their sensitive information. Additionally, Our Australian Study found that shopping increases users' ability to not respond to phishing emails. In contrast, Internet activities in Malaysian study increase users' likelihood to respond to phishing emails.

### 5.2 Similarities

In this section, we will discuss the similarities between cultures. Our study found that there are three latent variables have the same effect in different cultures. These latent variables are explained below.
Submissiveness has a positive impact on making users increase their likelihood to respond to phishing emails. Submissiveness impact did not change in different cultures. Submissiveness measures users' ability to oblige to others [1]. One explanation of submissiveness result is that phishing emails are designed to demand certain behaviour from users. It was expected that submissive users will respond to direct order. Despite differences in the dimension PDI which relates to respect power distribution between cultures, the effect of submissiveness is the same. It can be concluded that submissiveness variable has a higher effect than culture differences.

Email experience measures users' perceived experience with email. High email experience means that users are more able to encode and decode information in emails [4]. Our results show that users who are more experience with emails are more likely to not respond to phishing emails. This result is similar to our finding in Saudi Arabian study [2]. It is expected that experience in using email will increase users' ability to not respond to phishing emails. Expert users developed a baseline between trustworthy emails and fake emails. This experience helped users to recognise similar phishing email which they already identify as a phishing email.

The other types of Internet activities that are surfing and communicating agree with previous studies. Users who are more likely to use the Internet for surfing or communicating with others are more likely to be less careful about security. Since these activities does not require sharing sensitive information i.e., passwords. These users are more likely to be vulnerable to phishing emails as they might not know how to differentiate between real emails from fake ones. Our results in Malaysian study indicate that Internet activities have increase users' likelihood to respond to phishing emails despite their type of behaviour while using the Internet.

## 6. Conclusion

Phishing emails cause many damages and financial losses for both businesses and individuals. In the modern world, there are global organisations who hire people from different cultures and countries. Our research helps global organisations who employ staff from diverse countries and backgrounds to consider the culture of their staff as different cultures may behave differently. Certain measures implemented in one country may not be as effective in another one, as our results indicate. Employees from different cultures and countries have different vulnerabilities to security threats. Therefore, global organisations should consider these differences in their organisations training and security practises to improve their employees' protection. Our research gives an insight on these differences. For future research, the same questionnaire should be carried-out on different countries to measure its impact on users.

## References

[1] Allan, S. and P. Gilbert, *Submissive behaviour and psychopathology.* British Journal of Clinical Psychology, 1997. **36**(4): p. 467-488.

[2] Alseadoon, I., et al. *Who is more susceptible to phishing emails?: A Saudi Arabian study*. in *ACIS 2012: Location, location, location: Proceedings of the 23rd Australasian Conference on Information Systems 2012*. 2012. Geelong, VIC, Australia: ACIS.

[3] Alseadoon, I.M.A., *The impact of users' characteristics on their ability to detect phishing emails*. 2014, QUT: Brisbane, Australia.

[4] APWG. *APWG | Unifying The Global Response To Cybercrime* <https://apwg.org/>. 2019 [cited 2019 21/6].

[5] Carlson, J.R. and R.W. Zmud, *Channel expansion theory and the experiential nature of media richness perceptions.* Academy of management journal, 1999. **42**(2): p. 153-170.

[6] Cuchta, T., et al. *Human Risk Factors in Cybersecurity*. in *Proceedings of the 20th Annual SIG Conference on Information Technology Education*. 2019. ACM.

[7] Daft, R.L. and R.H. Lengel, *Organizational information requirements, media richness and structural design.* Management science, 1986. **32**(5): p. 554-571.

[8] Dhamija, R., J.D. Tygar, and M. Hearst. *Why phishing works*. in *Proceedings of the SIGCHI conference on Human Factors in computing systems*. 2006. ACM.

[9] Google. *Google Forms: Free Online Surveys for Personal Use* <https://www.google.com/forms/about/>. 2019 [cited 2018 2/5].

[10]Hofstede, G., *Culture's consequences: International differences in work-related values*. Vol. 5. 1984: sage.

[11]Insights, H. *Malaysia* - Hofstede Insights* <https://www.hofstede-insights.com/country-comparison/malaysia/>. 2019 [cited 2019 20/10].

[12]Insights, H. *Saudi Arabia* - Hofstede Insights* <https://www.hofstede-insights.com/country/saudi-arabia/>. 2019 [cited 2019 20/10].

[13]Insights, H. *Australia - Hofstede Insights* <https://www.hofstede-insights.com/country/australia/>. 2019 [cited 2019 20/10].

[14]Jain, A.K. and B.B. Gupta, *Phishing detection: analysis of visual similarity based approaches.* Security and Communication Networks, 2017. **2017**: p. 20.

[15]Kumaraguru, P., et al. *School of phish: a real-world evaluation of anti-phishing training*. in *Proceedings of the 5th Symposium on Usable Privacy and Security*. 2009. ACM.

[16]Likert, R., *A technique for the measurement of attitudes.* Archives of psychology, 1932.

[17]McKnight, H., C. Kacmar, and V. Choudhury. *Whoops... did I use the wrong concept to predict e-commerce trust? modeling the risk-related effects of trust versus distrust concepts*. in *System Sciences, 2003. Proceedings of the 36th Annual Hawaii International Conference on*. 2003. IEEE.

[18]Phishingbox. *Phishing Facts | Statistics on Phishing and other Cyber Threats* <https://www.phishingbox.com/resources/phishing-facts>. 2019 [cited 2019 23/7].

[19]Sheng, S., et al. *Anti-phishing phil: the design and evaluation of a game that teaches people not to fall for phish*. in *Proceedings of the 3rd symposium on Usable privacy and security*. 2007. ACM.

[20]Xiujuan, W., et al. *Detecting Spear-phishing Emails Based on Authentication*. in *2019 IEEE 4th International Conference on Computer and Communication Systems (ICCCS)*. 2019. IEEE.

[21]Yang, Z., et al. *Phishing Email Detection Based on Hybrid Features*. in *IOP Conference Series: Earth and Environmental Science*. 2019. IOP Publishing.

**Ibrahim Mohammed Alseadoon** received his Masters from University of Wollongong (UOW), Wollongong, NSW, Australia in 2008 and PhD from Queensland University of Technology (QUT), Brisbane, QLD, Australia in 2014. He is currently an associate professor at University of Ha’il (UOH), Ha’il, KSA. He is an author of more than 6 articles in the field of Computer Security and Users’ Behaviour. He served as general chair and program committee chair for several conferences. In addition, he served as the co-chair of the International Conference on Recent Advances in Computer Systems (RACS-2015) and The 2nd National Computing Colleges Conference (NC3 2017), And Chair for International Conference in Cybersecurity (ICCS) held at UOH

**Mohd Fairuz Iskandar Othman** Ph.D. Senior Lecturer, Department of Computer Systems and Communication, Faculty of Information and Communication Technology, UTeM. He received his Ph.D. in Information Technology from Queensland University of Technology and a Master’s degree in Internetworking from the University of Technology, Sydney. His research interests include human behavioural issues in Information Security, IT Governance and Management, and other related topics in Computer Networks and Computer Security.