Turkish Journal of Computer and Mathematics Education *Vol.12 No.14 (2021), 1158 - 1164*

Research Article

DEVELOPMENT OF AN INTERNET RISKS ASSESSMENT USING A DIGITAL INTELLIGENCE QUOTIENT AND A COMMUNICATION-BASED MODEL

Chaichana Kulworatit [a], Somkiat Tuntiwongwanich [b*], Sirirat Petsangsri [c]

[a b* c] School of Industrial Education and Technology, King Mongkut's Institute of Technology Ladkrabang, Bangkok, Thailand
[a] 62603012@kmitl.ac.th, [b*] somkiat.tu@kmitl.ac.th, [c] sirirat.pe@kmitl.ac.th
[*] Corresponding author

Article History: *Received: 5 July 2021; Revised: 12 July 2021; Accepted: 14 July 2021; Published online: 9 August 2021*

Abstract: The purposes of this study were 1) to create an internet risks assessment using a digital intelligence quotient and a communication-based model, and 2) to improve the quality of such an internet risks assessment using the digital intelligence quotient and the communication-based model with a field test comprising Face Validity, Content Validity, Construct Validity and Reliability. The sample group included 400 specifically selected message receivers - all Thai digital natives. The research tool was the internet risks assessment using a digital intelligence quotient and a communication-based model that was developed by the researcher. It consisted of seven categories with 27 questions in total. Its reliability value was 0.85. The results of the research found that 1) the development of internet risks assessment using a digital intelligence quotient and a communication-based model had seven variants, and 2) the quality of the assessment contained Content Validity at 0.85, Reliability at 0.88, and Construct Validity - improved by the Exploratory Factor Analysis (EFA). The questions were categorised into seven sections comprising Digital Identity, Digital Safety, Digital Emotional Intelligence, Digital Rights, Digital Fear, Digital Greed, and Digital Unreasonable Decision.

Keywords: Assessment development, Digital intelligence quotient, Communication

1. Introduction

Nowadays, it is undeniable that the internet an important, if not vital, aspect of human life. Internet technology is the digital key that helps create and complete society in various dimensions, including daily life, education, business, etc. It is also the main driver of both the microeconomy and macroeconomy. However, there are some disadvantages to the internet, the most obvious being that it can be used to spread threats. According to the Official Annual Cybercrimes Report by Cybersecurity Ventures, an IT security magazine in the United States of America, it was forecasted that cybercriminal activity could cost the world's businesses and consumers 6 trillion US dollars in 2021, an increase from 3 trillion US dollars in 2015. This represented the immense transfer of economic wealth on the black market, which tends to attract certain entities to become cybercrime penetrators because it requires little investment but potentially immense profitability, more than the global trade of all major illegal drugs combined (Cybersecurity Ventures, 2020). Cybercriminals target both individuals and organisations in the public and private sectors. In 2018, cybersecurity spending was visibly increased in all aspects due to the advancement of technology. According to a report by Thailand's Computer Emergency Response Team (ThaiCERT), most cybersecurity incidents reported in Thailand in 2020 concerned malicious codes - which involve a script that is intended to cause security breaches or damage to a system in order to spy on and/or steal users' information. The second most prevalent cybersecurity incident involved internet fraud - which includes crimes such as using others' personal information without permission, piracy, identity theft, or any activities that take advantage by disguising as someone else (The European Computer Security Incident Response Team Network, 2003). Masquerading as a trusted entity and tricking a victim into opening an email, URL, instant message, or text message to steal the victim's data is called Phishing. The practice originated sometime around the year 1995 and still exists now on many channels including mobile phones, websites, and social media such as Facebook, Twitter, etc. (Pongpon, 2018).

In the current digital era, people around the world connect to the internet easily on their smartphones or tablets. In fact, many tasks are done with a simple click, including searching for information, enjoying media content, conducting financial transactions, etc. However, everything has two sides, meaning there are also disadvantages to the convenience of using the internet. As the number of connected devices is increasing in cyberspace, cybercrimes are increasing as well, including privacy breaches, personal information theft, cyber-attacks, loss of safety in life and property, etc

The Digital Intelligence Quotient (DQ) is the sum of the social, emotional, and cognitive abilities that enable individuals, like digital citizens, to face challenges and adapt to the demands of life in the digital world. DQ can be further deconstructed into eight key areas: 1) Digital Identity, 2) Digital Use, 3) Digital Safety, 4) Digital Security, 5) Digital Emotional Intelligence, 6) Digital Communication, 7) Digital Literacy, and 8) Digital Rights. DQ also has three levels: 1) Digital Citizenship, 2) Digital Creativity, and 3) Digital Entrepreneurship.

According to David Berlo's SMCR Model of Communication, there are four components to describe the communication process including sender, message, channel and receiver. These are also the components of phishing. The attackers, as senders, build their credibility to phish successfully. The messages they send attract victims' interest, demand, or expectation. The attackers choose channels, predominantly digital media, to spread their phishing quickly and connect to as many people as possible. Finally, the receivers who have fear, greed, curiosity and irrational decision-making may fall victim to phishing easily. Phishing in digital media is one of the biggest cybercrimes in the world. Thailand is a target of both foreign and local attackers. Software alone is not sufficient to safeguard users from phishing as the attackers keep creating strategies to deceive victims rather than penetrating the system. Thus, this researcher was interested in developing an internet risks assessment focusing on communication to find the right tool to assess internet risks. The results should be advantageous for other articles of research as well.

2. Research Purposes

- To create the internet risks assessment using a digital intelligence quotient and a communication-based model.
- To improve the quality development of the internet risks assessment by using a digital intelligence quotient and a communication-based model with a field test including Face Validity, Content Validity, Construct Validity and Reliability.

3. Framework

The research "Development of an Internet Risks Assessment Using a Digital Intelligence Quotient and a Communication-based Model" used the concept of a Digital Intelligence Quotient of Na-nan and a Model of Communication by Berlo, together with literature about cybercrimes and phishing incident reports in Thailand.

4. Population and Sampling Group

The population of this research was message receivers - all Thai digital natives, aged between 18-36 years. The message receivers generally used the internet for five consecutive years. The population totalled 4,387,062 people (ITU, 2013). The researcher collected information from the digital natives who lived in Bangkok, where 85.3% of the population generally used the internet - the highest among all regions (National Statistics Office Thailand, 2019). The in this study were analysed with SPSS statistic software. The details are specified as follows:

- General information about respondents such as age, sex, income, education, etc. was analysed with Descriptive Statistics to find the frequency, percentage, average and standard deviation.
- The variants of the assessment were analysed with the Exploratory Factor Analysis.
- Each question was analysed.
- The researcher also calculated using Cronbach's Alpha Coefficient to find the reliability of the tool.

5. Research Process

This research employed scale development research using quantitative methods. The study was divided into 2 phases. The first phase was the development of the internet risks assessment using a digital intelligence quotient and a communication-based model, while the second phase was the quality improvement of the internet risks assessment.

- The development of the internet risks assessment is a study based on research with the purpose of "Creating an internet risks assessment using a digital intelligence quotient and a communication-based model". The researcher collected information from documents, education books, researches related to cybercrimes, and reports of phishing incidents in Thailand. The researcher applied the collected information to the assessment using the 5-point Likert scale, which consisted of Strongly Agree, Agree, Neither Agree nor Disagree, Disagree and Strongly Disagree.
- The quality improvement of the internet risks assessment is a study based on the research purpose of "Improving the quality development of the internet risks assessment using a digital intelligence quotient and a communication-based model with a field test including Face Validity, Content Validity, Construct Validity and Reliability". The test processes were as follows

5.1. Face Validity

The researcher submitted the internet risks assessment using digital intelligence quotient and communication-based model to a professor at the School of Industrial Education and Technology at King Mongkut's Institute of Technology Ladkrabang for suggestions on language correction and content accuracy. The researcher then made changes following the suggestions provided.

5.2. Content Validity

The researcher took the internet risks assessment using digital intelligence quotient and communication-based model to five experts in computer system security to recheck the content validity. The researcher used the results to calculate the Content Validity Index - both item content validity index (I-CVI) and scale content validity index (S-CVI). The researcher then made a change for tool accuracy following their suggestions.

5.3. Construct Validity

The researcher took the internet risks assessment using a digital intelligence quotient and a communication-based model, which had passed the Face Validity and Content Validity processes, to 30 message receivers identical to the sampling group for responses. The researcher then used the results to calculate the Reliability of the tool and analysed each item. The researcher chose the items which scored the Item-Total Correlation at +0.30 or more to create the assessment. Finally, the researcher took the finished assessment to the sampling group of 400 people for responses. The results from the sampling group were applied with Exploratory Factor Analysis to find the correlation between variants and to reduce the number of questions in the assessment by choosing only the questions with Factor Loading of 0.03 for use in the assessment.

6. Research Results

The researcher extracted variants from related researches and literature while developing the internet risks assessment using a digital intelligence quotient and a communication-based model. The variants included two variants of senders who were faking the identities of important people and building credibility, and seven variants of messages involving Digital Identity, Digital Safety, Digital Emotional Intelligence, Digital Rights, Digital Fear, Digital Greed, and Digitally Unreasonable Decision. With these, the researcher was able to pose 35 questions.

For Face Validity, the researcher revised the questions following the suggestions of a professor at the School of Industrial Education and Technology at King Mongkut's Institute of Technology Ladkrabang. The researcher took the assessment to five experts in computer system security to recheck the Content Validity. The experts gave a score for each question ranging from 1 to 4 points. The results were used to calculate the Content Validity Index (CVI) - both item content validity index (I-CVI) and scale content validity index (S-CVI). The I-CVI score was 0.6-1.0, and the S-CVI was 0.89. The researcher corrected the language used in the questions for accuracy following the suggestions of the experts. The questions were also reduced from 35 to 28 and categorised into seven sections as follows.

Section 1 - Digital Identity totalled 5 questions (Questions 1-5)

Section 2 - Digital Safety totalled 4 questions (Questions 6-9)

Section 3 - Digital Emotional Intelligence totalled 3 questions (Questions 10-12)

Section 4 - Digital Rights totalled 5 questions (Questions 13-17)

Section 5 - Digital Fear totalled 5 questions (Questions 18-22)

Section 6 - Digital Greed totalled 3 questions (Questions 23-25)

Section 7 - Digitally Unreasonable Decision totalled 3 questions (Questions 26-28)

A five-point Likert scale was applied to the questions ranging from 1 to 5: 5 points for Strongly Agree and 1 point for Strongly Disagree. The higher scores meant higher internet risks.

The reliability of the internet risks assessment using a digital intelligence quotient and a communication-based model was tested using a sampling group of 30 people identical to the research population. The researcher calculated the score of Item-Total Correlation (Farnsworth, 1928), which was equal to 0.85, and the Cronbach’s Alpha Coefficient for each section as follows.

Section 1 - Digital Identity at 0.87

Section 2 - Digital Safety at 0.88

Section 3 - Digital Emotional Intelligence at 0.92

Section 4 - Digital Rights at 0.85

Section 5 - Digital Fear at 0.88

Section 6 - Digital Greed at 0.91

Section 7 - Digitally Unreasonable Decision at 0.79

The quality improvement of the internet risks assessment using a digital intelligence quotient and a communication-based model was done by using a sampling group of 400 people. The reliability score was equal to 0.85, and the Cronbach's Alpha Coefficient for each section was as follows.

Section 1 - Digital Identity at 0.85

Section 2 - Digital Safety at 0.88

Section 3 - Digital Emotional Intelligence at 0.80

Section 4 - Digital Rights at 0.84

Section 5 - Digital Fear at 0.90

Section 6 - Digital Greed at 0.88

Section 7 - Digitally Unreasonable Decision at 0.75

The scores for Item-Total Correlation on each question were between 0.25 and 0.52, except for question A09 "You will immediately trust the information delivered by people you know" which scored the Item-Total Correlation at only 0.08. The assessment was considered to have an item-total correlation (Jirojanakul & Skevington, 2000).

The construct validity of the internet risks assessment using a digital intelligence quotient and a communication-based model was applied with the Exploratory Factor Analysis (EFA) using the rotation method of Varimax with Kaiser Normalisation. The data from a sampling group of 400 people were used for calculation. The preliminary results found that the KMO and Bartlett's Test measure of sampling adequacy was 0.65 and Bartlett's Test of Sphericity was $\chi 2 = 5733.96$, p 0.000. This meant all variants were suitable for analysis (Sudarat, 2015).

Table.1. Factor loading value and categorisation of questions.

Section		**Factor Loading**
Section 1 (4 questions)		
A03	You always use your real name to build a profile.	0.759
A02	You always use your own photo to create a profile picture.	0.729
A04	You immediately ignore the comments that oppose your thoughts in digital media.	0.684
A01	You stop communication immediately with those who display wrong behaviour in digital media.	0.650
Section 2 (4 questions)		
A07	You will avoid or immediately stop communication when you feel threatened by digital media.	0.749
A05	You will avoid or immediately stop communication when you are attacked by speech or an image in digital media.	0.710
A06	You will avoid or immediately stop communication when you are asked about personal information in digital media.	0.682
A08	You will avoid unconventional content or websites that promote nudity every time you use digital media.	0.625

Section 3 (3 questions)		
D02	You will reply immediately to a post you feel sad about with a cheer-up message.	0.749
D01	You will always offer suggestions to a post that is asking for help.	0.710
D02	You will always post a message to notify friends or acquaintances that you feel unimportant every time you use digital media.	0.682
Section 4 (5 questions)		
C02	You always refer to the source every time you have to use other people's achievements.	0.749
C05	You will always avoid breaching privacy and the law every time you share information in digital media.	0.710
C03	You will never download software or movies with copyright.	0.682
C04	You will never post a comment as someone else, any time you use digital media.	0.681
C01	You will always be thinking about the social impact of your posts on digital media.	0.672
Section 5 (5 questions)		
B03	You always feel afraid when someone says they have secret photos of you.	0.887
B04	You always feel afraid when you receive a message like "Your account is subject to money laundering".	0.765
B01	You will always make a backup every time you use the computer.	0.675
B05	You always feel afraid to see a message like "High amount on your credit card debt".	0.637
B02	You always feel afraid every time you are asked to lend someone money.	0.629
Section 6 (3 questions)		
B08	You will feel special every time you receive a message that says specials are made just for you.	0.723
B06	You will always provide personal information such as your name, address and telephone number when you come across a website that promises rewards.	0.662
B07	You will press the shortcode (USSD) every time to win big with agencies you don't know.	0.599
Section 7 (3 questions)		
C08	You will always use the company's email account for any kind of online registrations	0.850
C07	You will always click a link when you want to search for a file to download.	0.768
C06	You will write down the password in a place that is easy to find every time you want to remember it.	0.675

7. Conclusion and Discussion

The development of the internet risks assessment using a digital intelligence quotient and a communication-based model was initiated by the researcher's collection of literature and other researches related to cybercrimes and phishing incidents in Thailand. 35 questions were initially posed. The assessment passed the improvement on accuracy and language usage following the suggestions of a professor at the School of Industrial Education and Technology at King Mongkut's Institute of Technology Ladkrabang and five experts in computer system security. The researcher was advised to reduce the number of questions from 35 to 27 and categorise them into seven sections. The assessment passed the preliminary test with a sampling group of 30 people before being tested with a real sampling group of 400 people. The reliability value of the assessment following Cronbach's Alpha Coefficient was equal to 0.85. A new tool with a value of Cronbach's Alpha Coefficient at more than 0.70 was considered to have Item-Total Correlation (Nunnally & Bernstein, 1994).

Content validity was rechecked by five experts in computer system security. The value of the Content Validity Index (CVI) was 0.87 - which was considered acceptable (Polit & Hungler, 1999). This signified that the assessment that was improved by the experts had Content Validity and could be used for real assessment.

For the Construct Validity, the results of the analysis in this study concerning the risks of being phished in digital media using a communication-based model could be categorised into seven sections as follows.

Section 1 was the section with the most questions - 4 questions in total. As all questions related to identity verification, Section 1 was named Digital Identity.

Section 2 had 4 questions in total. As all questions related to internet safety, Section 2 was named Digital Safety.

Section 3 had 3 questions in total. As all questions related to the users' emotions, Section 3 was named Digital Emotional Intelligence.

Section 4 had 5 questions in total. As all questions related to personal rights, Section 4 was named Digital Rights.

Section 5 had 5 questions in total. As all questions related to the users' fears, Section 5 was named Digital Fear.

Section 6 had 3 questions in total. As all questions related to the users' greed, Section 6 was named Digital Greed.

Section 7 had 3 questions in total. As all questions related to unreasonable decision-making, Section 7 was named Digitally Unreasonable Decision.

Following the analysis results, the question "You will trust immediately the information delivered by people you know" (A09) scored the Item-Total Correlation at only 0.08 were cut from the assessment. This represented that question A09 "You will trust immediately the information delivered by people you know" had a variety of answers which led to a low score of Item-Total Correlation and was likely not related to other questions. After cutting question A09, the total number of questions in the assessment remained at 27.

The internet risks assessment using a digital intelligence quotient and a communication-based model passed the development and improvement in many criteria including Face Validity, Content Validity, Construct Validity and Reliability was considered acceptable. Others with a desire to refer to this assessment can be confident in its efficacy.

8. Suggestions

- The internet risks assessment using a digital intelligence quotient and a communication-based model was studied using a specific target group. For further study, the researcher or interested people should consider changing the target group and revising the question to meet the target group's characteristics in order to calculate the reliability again.
- The researcher was advised to conduct a qualitative research study to bring insights to integrate the assessment, together with studying more related literature.

References

Cybersecurity Ventures. (2018). *2019 Official Annual Cybercrime Report*. Retrieved November 25, 2020, from https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf

Farnsworth, P. R. (1928). The Spearman-Brown prophecy formula and the Seashore tests. *Journal of Educational Psychology*, 19(8), 586-588. https://doi.org/10.1037/h0070293

Inter Telecommunication Union [ITU]. (2013). *Measuring the information society*. Geneva: . Retrieved November 25, 2020, from https://www.itu.int/en/ITU-D/Statistics/Documents/publications/anapub/Youth_2008.pdf

Jirojanakul, Pragai & Skevington, Suzanne. (2010). Developing a quality of life measure for children aged 5-8 years. *British Journal of Health Psychology*. 5. 299 - 321. 10.1348/135910700168937.

Na-Nan, K., Roopleam, T., and Wongsuwan, N. 2019. "Validation of a digital intelligence quotient questionnaire for employee of small and medium-sized Thai enterprises using exploratory and confirmatory factor analysis." *Emerald Publishing Limited*. 49(5) : 1465-1483.

National Statistics Office Thailand. (2019). *The 2019 Household survey on the use of information and communication technology*. Retrieved Octorber 8, 2020, from http://www.nso.go.th/sites/2014/DocLib13/ด้าน ICT/เทคโนโลยีในครัวเรือน/2562/Pocketbook_2562.pdf

Nunnally, J.C. and Bernstein, I.H. (1994) *The Assessment of Reliability*. Psychometric Theory, 3, 248-292.

Polit, D. F., & Hungler, B. P. (1999). *Nursing research: Principles and methods (6th ed.)*. Philadelphia: Lippincott.

Pongpon Pawasut. (2018). *An In-dept of the Social Engineering attarcks of generlation y in Bangkok and Metropolitan*. Master of Science Program, Thammasat University.

Sudarat sangkaew. (2015). *Scale Development of Self-Disclosure Through Online Social Network (Facebook)*. Industrial Technology Lampang Rajabhat University Journal. 8(2) 101 - 111.

Thaicert (Thailand Computer Emergency Response Team). (2020). *Threat statistics 2563*. Retrieved Octorber 8, 2020, from https://www.thaicert.or.th/statistics/statistics.html

The European Computer Security Incident Response Team Network. (2003). *WP4 Clearinghouse Policy*. Retrieved November 5, 2020, from http://www.ecsirt.net/cec/service/documents/wp4-clearinghouse-policy-v12.html