`

Priming Intervention Improves Identification of Authentic QR Codes

Submitted by:
Lee Cher Chye, Muhammad Kashfun Nazir Bin Mohd Ali

Project Supervisor

Professor Pieter Hartel

(Singapore University of Technology and Design, Singapore)

Master of Science in Security by Design (MSSD)

A project submitted to the Singapore University of Technology and Design in fulfilment of the requirement for the course of Cyber Crime

5529 words

Abstract

People tend to trust each other and to easily use the information presented to them. This makes them vulnerable to social engineering attacks through Quick Response (QR) codes. This study investigated the effectiveness of intervention that aim to protect users, through priming cues to raise awareness about the dangers of social engineering attacks via QR codes. A sample of graduate students in Singapore University of Technology and Design (SUTD).

This study provided a quantitative review on the effect of priming intervention when identifying authentic QR codes from fictitious and if there were any effect differences of priming intervention between younger adults and older adults. The results were discussed in this study where the effect of priming intervention when identifying authentic QR codes from fictitious was significant, but the effect was not significantly different between younger adults and older adults. We conclude the findings and proposed possible future research.

Keywords: QR code, priming intervention, age difference

Introduction and Literature Review

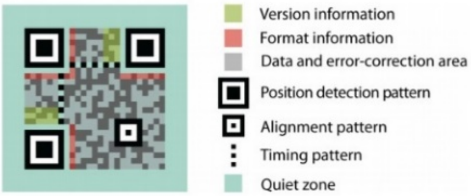
Quick Response (QR) codes are flat 2-Dimensional (2-D) codes that visually encode bits of information represented as black square dots placed on a white square grid. QR codes, is an extension of the 1-dimensional (1-D) barcode commonly used in retail and production. Unlike standard Universal Product Code (UPC) barcodes, QR code is a matrix code, with its arrangement of its dark and light elements in columns and rows (Krombholz et al., 2015).

Figure 1
UPC Bar code structure
(Krombholz et al., 2015)

A1234567890A

The QR code itself is simply an array of bits to be identified by a scanner. Bits are reserved for the scanner to be able to identify and orient the image, as well as for version and format information (Figure 2). The remaining bits are used to encode the message, and the specific amount of available space leftover is dependent on the version of the QR code, which indicates the number of bits per row/column, and the level of error correction, which introduces redundancy. The most information dense QR codes used today can store just under 3,000 bytes of raw data (Kieseberg et al., 2010).

Figure 2
QR code structure
(Kieseberg et al., 2010)



QR codes, capable of encoding the same amount of data in about one-tenth the space of 1-D barcodes, present a more space-efficient way of presenting data. QR codes, originated from Japan, were used to track automotive parts quickly in order to speed up car production. The data in a QR code can be accessed by taking a picture of the QR code and processing it with a QR code reader.

Popular commercial uses of QR codes now include URL redirection, payment information exchange, and electronic flight tickets. However, there are now more widespread use as convenient methods of sharing and transmitting data. Other uses include Advertising, Mobile Payments, Access Control, Augmented Reality & Navigation (Krombholz et al., 2015).

The threat is that the QR code could have a malicious URL embedded in it that would lead to dubious sites which could contain malware — short for malicious software — that could be installed on your mobile device. Malware can compromise your device's software and share sensitive information with cybercriminals. Some ways that malwares pose a threat include making your calendar, contacts, and even credit card information available to criminals, stealing your Facebook, Google, and other passwords and tracking your location for criminal purposes and infecting your device with malware that can disable it.

The security and privacy threats that QR codes pose are real, however documented cases of abuse are low, as QR Codes are just beginning to catch on with consumers. As the trend in usage increases, QR codes could become a popular tool for cybercriminals to exploit unsuspecting users. The key is to do what you should do when faced with risks: Take precautions!

QR Code Security

The security of QR codes is not in the code itself but the human factor, the ability to read and identify the Uniform Resource Locator (URL). In a study, Krombholz et al. (2015) discussed that the QR code does not provide any sort of security. Their result showed that 11 out of 12 QR code reader applications do not use any sort of security services such as Google Safe browsing or malicious URL detection tools which could provide effective security measures. Their study also discussed that since QR codes not being human-readable, the way to identify if a QR code is malicious or authentic is through the URL displayed upon scanning. It is then up to the user to decide if the link is malicious and if the user should visit the link.

QR Code Phishing

With the growing popularity of the usage of QR codes due to its convenience, there is also a rise in phishing cases. Yong, Chiew and Tan (2019) said that a QR code could easily be manipulated into a malicious version by either replacing the entire QR code (e.g. pasting over another QR code) or adding black modules to the white ones, which could be easily done by using a pen or other tools. Their study discussed countermeasures which ranged from software-based to user-centred. Software-based countermeasures proposed focused on digital signing or encryption of data. User-centered countermeasures referred to "user awareness and education of the danger of malicious QR codes". Their study concluded that software-based countermeasures are still inadequate and that user-centred countermeasures are still a better solution to QR code phishing.

Vidas et. al. (2013) found that 85% of people who scanned a QR code visited the website associated subsequently through a surveillance experiment. In their experiment, 4 differently designed flyers were distributed. First design only had a QR code with no words or images, second had QR code with usage instructions, the third had a QR code with words advertising a Social Network Study for interested participants to scan the QR code, the last design had the same word advertisement as the third but instead of a QR code, a link to the website was printed. Vidas et. al. found that the flyer with only QR code had the most participants. Their results suggested that curiosity was the largest motivating factor for scanning QR codes. Due to people's curiosity, attackers can position QR codes under false pretences and entice users to scan the codes and lead them to malicious/phishing websites.

Although QR phishing is a threat, researchers have yet to come up with an effective and evidence-based intervention that is targeted towards training people against this specific threat.

With its proven psychological and behavioural effects, this study will explore the inclusion of priming in designing an effective QR phishing intervention in the next section.

Priming Intervention

Priming refers to an intervention method by external cues that can affect one's behaviour or/and processing of information. An external cue could be in words or graphics that represent a concept, such as a poster or banner (Papies, 2016).

In a study by Doyen, Klein, Pichon and Cleeremans (2012), an experiment was carried out to see if the participants would walk slower when given a priming intervention. The prime implemented in the experiment consisted of 30 scrambled sentences, all including words related to the concept of "slow". The participants in the priming group were tasked to rearrange the 30 scrambled sentences in the correct order and strike out the word that would not fit in the sentence. Each sentence consisted of four to five words and no time limit was given. The speed of the participants from both primed and non-primed groups were measured. The study found a significant difference in walking speed and that the primed group's participants were found to have slowed down their walk.

However, in Junger, Montoya and Overink's (2017) study, priming intervention was not found to be very effective. Their study investigated the effectiveness of two interventions which were aimed to guard users from social engineering attacks. The priming was done through warnings against disclosing personal information and raising awareness of social engineering's dangers. Its results showed that a high percentage of the users disclosed personal information and the difference between prime group and non-prime group were negligible. Analysis of the results also found that neither intervention method influenced the degree of disclosure.

In another study, the efficacy of subliminal priming was tested. The study wanted to find if priming disrupted the reading process and if it affects users' image selection (Caraban, Karapanos, Teixeira, Munson & Campos, 2017). Participants were tasked to read a short sentence which referred to at least three concepts. After which, they were to choose one of three images. Each image reflected one of the concepts in the sentence read earlier. The objective was to see if priming one of the concept, would influence participants to choose the relevant image. The results showed that participants who did not undergo priming, chose the primed concepts 28% of the time while those who underwent priming and chose the primed concepts was significantly higher ($p < 0.05$) at 42%.

The study by Caraban et. al. showed that priming intervention is significant, and we would like to test that in this study. We hypothesise that: Participants who has undergone the priming intervention will score higher in awareness/knowledge of fictitious QR codes compared to participants in the non-intervention condition.

Age differences in Priming intervention

It was found by Stein et. al. (2002) that testing the priming effect between young and old adults showed that the younger adults scored significantly higher than older adults. In this study, younger and older adults' memory were tested before and after priming intervention. Through the photo recall task and dot location task, the younger adults were observed to have performed better than the older adults before priming intervention was significantly higher after priming intervention. However, priming intervention was observed to be of negligible effect on the older adults.

It is a common assumption that the younger generation is more aware of technology and its uses as compared to the older generations. In the study done by Mendelson and Bergstrom (2013), the assumption was found not too far from the truth based on the study's findings. The study examined QR code awareness, knowledge and usage by age across three groups, younger adults, middle-age adults and older adults. The results showed that younger adults scored highest in all three segments, awareness, knowledge and usage. Part of the results showed the likeliness that the younger adults would scan a QR code, on a billboard, poster or a sign, was almost double that of middle-age adults. Despite that, the study also found that middle-age adults' use of QR codes are comparable to that of younger adults.

Based on findings by Stein et. al. (2002) and Mendelson and Bergstrom (2015), we hypothesised that younger adults (participants 35 years old or younger) who have undergone priming intervention will score higher in awareness/knowledge of fictitious QR codes compared to older adults (participants over 35 years old) who have undergone priming intervention.

The Current Study

The review of literature has shown that QR code phishing a new and rising trend. In the current study, it was approached by the formation of the Research Question.

Research Question
To what extent does priming intervention improve one's ability to distinguish "fictitious" from "authentic" Quick Response (QR) Codes?

Research Hypotheses
This study tested two hypotheses through a survey.

Hypothesis One
Participants who has undergone the priming intervention will **score higher** in awareness/knowledge of fictitious QR codes **compared to** participants in the non-intervention condition

Hypothesis Two
Younger adults (participants 35 years old or younger) who have undergone priming intervention will **score higher** in awareness/knowledge of fictitious QR codes **compared to** older adults (participants over 35 years old) who have undergone priming intervention.

Method

We employed an online survey for participants to complete. Results of the online survey were recorded anonymously, where no personal identification was recorded.

Participants

The survey consisted of a declaration of consent and 12 questions (Table 2), collecting participants' age group, gender, citizenship, five sets of two QR codes questions, where participants were expected to choose either an "authentic" or "fictitious" QR code and follow-up questions.

Amongst the 51 participants, 8 were females, 39 were males and 4 preferred not to say their gender. The age groups of the participants consisted of 29 younger adults, 20 older adults and 2 preferred not to say their age. We categorised the participants into two age groups: younger adults aged 35 and below and older adults aged 36 and above.

Table 1
Sample Demographics

Sample Demographics ($N = 51$)

Variable	**% of sample**
Gender	
Male	76.5
Female	15.7
Prefer not to say	7.8
Age Groups	
Younger adults (<36)	56.9
Older adults (>35)	39.2
Prefer not to say	3.9

Note: The percentages presented are rounded off to one decimal place and may not necessarily add to 100%

Procedure

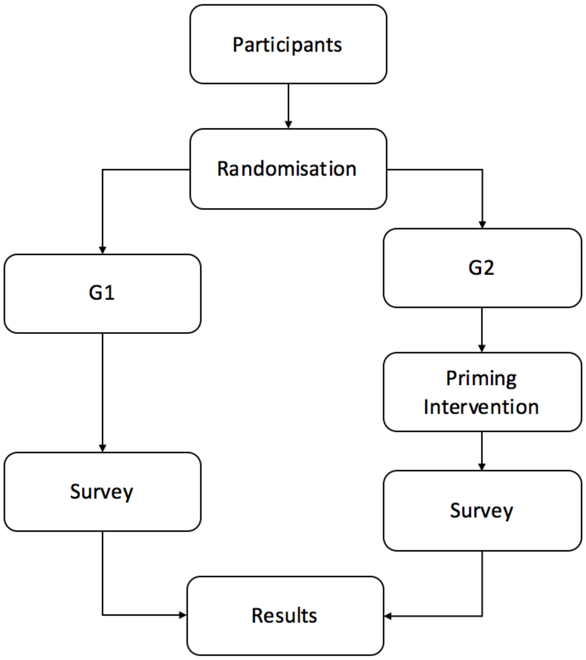
The survey was carried out in a classroom setting, over two sessions, one working day after the other, where a total of 51 students from SUTD's Master of Science in Security by Design (MSSD) course participated. The survey was designed and carried out on *Limesurvey – an online statistical survey platform*. We flashed the URL of the online survey for the participants to access from their laptops individually. Each participant was required to use their smartphone to scan the QR codes in the survey. Those without access to smartphones with the ability to scan QR codes (2 MSSD students) were lent a smartphone to scan the QR codes by the investigator(s).

Before the start of the survey, the participants were briefed on the purpose of the survey; to study the awareness/knowledge of the participants in identifying "authentic" and "fictitious" QR codes. It was emphasised that no personal identification information was collected and that all results collected would be kept confidential and only accessible by the investigators. They were also informed that participants were given the option not to disclose their age and gender by selecting the option "prefer not to say" when asked.

At the beginning of the survey, the participants were able to read the declaration of consent. It was made known to the participants that by participating in the survey, they have agreed on the informed consent and are able to request for withdrawal from the survey at any time by contacting the investigators.

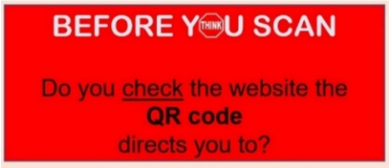
The survey was programmed to randomly select participants shown in procedure flow chart (Figure 3) and split them into two groups: without priming intervention (G1) and with priming intervention (G2). We had no influence in choosing the assignment of the participants to the groups.

Figure 3
Procedure Flow Chart



Other than having the graphical intervention shown, all questions in the survey were the same for both groups of participants. Neither groups had any additional question than the other.

Figure 4
Graphical intervention



BEFORE YOU SCAN

Do you check the website the QR code directs you to?

After the declaration of consent, participants in G2 were shown the graphical intervention (Figure 4). There was no question asked on this page. Participants in G1 did not see this page and were directed to the first question.

The first question was with regards to age. Participants were asked to choose the age range option they belong to. They were not asked to specify their age. They were also given an option "prefer not to say" should they not want to disclose their age. The second question was with regards to gender. Participants were asked to choose one of the three options: male, female or prefer not to say. The third question was with regards to citizenship. Participants were asked to identify if they are Singaporean.

The next five questions were to get the participants to identify the "authentic" QR code. In each question, participants were presented with a set of two QR codes, one "authentic" and the other "fictitious". All the QR codes were created with the use of free online QR code generator. Each QR code were tagged to a URL as shown in Table 2. There were no duplicates in any of the sets.

Table 2
QR code tagged URLs

No.	Authentic QR Codes	Fictitious QR Codes
1	cpf.gov.sg	cp5.gov.sg
2	docs.google.docs	d0cs.google.com
3	monkey-survey.com	mokey-survey.com
4	go.gov.sg/mohmarch	go.g0v.sg/mohmarch
5	dropbox.com	dropbox..com

The participants were then asked follow-up questions to understand their reason(s) behind their choices of QR codes. At the end of the survey, the participants were shared with bit-sized information to educate them on QR codes. This information had no impact to the survey results and were purely for the education of the participants.

Table 3
Questions in survey

No.	Question
1	Informed Consent
1a	Graphical intervention for G2 participants
2	What is your Age?
3	What is your gender?
4	What is your citizenship?
5	Which do you think will direct you to the "authentic" website?
6	Which do you think will direct you to the "authentic" website?
7	Which do you think will direct you to the "authentic" website?
8	Which do you think will direct you to the "authentic" website?
9	Which do you think will direct you to the "authentic" website?
10	How often do you scan QR codes?
11	What purpose(s) do you normally scan QR codes?
12	In the five(5) previous questions, did you always check the website the QR code directs you to?
13	How do you determine whether a QR code is "authentic"?

Collection of Data

The data for this study was obtained from an online survey – hosted on LimeSurvey platform – where the participants from MSSD were given a URL link to complete the survey. This online survey adopted the Random Generator, that helps to randomize the survey each participant received. The use of rand(1,2) function as the Random Generator, has a known limitation which the team was not aware when we set up this online survey. This function will return a pseudo random value. The pseudo random value isn't really random as it is often based on things such as the current date and time. The (1,2) limits implemented in the rand() function also resulted in the skew, whereby 36 the survey participants receiving survey number 1 (without priming intervention) and 15 of the participants receiving survey number 2 (without priming intervention). The total number of survey participants is 51. To circumvent this skewness (36:15), there would be a need to have a larger group of respondents which is a challenge for this study as the survey participants in our survey are scoped to the MSSD students in SUTD.

Data Pre-processing

The data pre-processing consisted of deleting incomplete surveys and considering only those completed survey. Further, from the data received, information that was not impacting the study such as Gender, Citizenship and additional information like prior experience with QR code were excluded.

Classification of Data

The data were classified into simple variables for the conduct of analysis. Since the data collected were from two sets of surveys, the responses received from the participants were distilled into two groups: 1. without priming intervention (NOTPRIMED) and 2. with priming intervention (PRIMED). The choices made by the participants for the 5 sets of QR codes were tabulated as "0" when they get the wrong QR code and "1" when they get the correct QR code. The age of the participants was categorized with the younger participants (35 years old and below) were tabulated as "YOUNG" and the older participants (36 years old and above) were tabulated as "OLD" as shown in Table 4.

Table 4
Survey Variables

CATEGORY	Variables	
SURVEY	PRIMED	NOTPRIMED
QR1	WRONG = 0	RIGHT =1
QR2	WRONG = 0	RIGHT =1
QR3	WRONG = 0	RIGHT =1
QR4	WRONG = 0	RIGHT =1
QR5	WRONG = 0	RIGHT =1
AGE	YOUNG	OLD

Results

Hypothesis One

To test our first hypothesis, independent t-test was conducted to compare whether there was any significant influence of priming intervention on the selection of the QR codes by the participants. If the p-value recorded was less than $\alpha = 0.05$, then we are 95% confident that there was a significant impact on priming intervention on choosing the correct QR code. Hence in this study, we are testing for the Hypothesis (H_0) on whether means of the different variables are the same (ie. means for those with priming intervention and those without priming intervention).

This study found that participants who has undergone the priming intervention will **score higher** in awareness/knowledge of fictitious QR codes **compared to** participants in the non-intervention condition.

Quantitative Analysis

Running the means analysis for QRtotal score, it shows the means is 4.49 with a standard deviation (sd) of 1.05 for the sum of all the correct QR codes selected as shown in Table 1. The study will test if the participants who have undergone priming intervention will achieve higher total QR score (QRtotal). This is compared with the results achieved by participants who did undergo priming intervention.

Table 5
Means Table

	mean	sd	skew	kurtosis
SURVEY	1.31	0.47	0.78	-1.42
AGE	1.57	0.50	-0.28	-1.96
QRtotal	4.49	1.05	-1.87	2.23

From Table 5, the distribution with a Skew of |1.87| and Kurtosis of |2.23|, was sufficiently normal for conducting a t-test. (which is within the scope of rule for Normality of Skewness <│2│ and Kurtosis <│9.0│).

Table 6
Welch Two Sample t-test

Data: QRtotal by SURVEY	Result	
t	-3.6726	
df	34	
p-value	0.0008184	
Alternative hypothesis: True different in means is not equal to 0 (95% confidence interval)	-1.153915	-0.331799
Mean in group PRIMED	5.000000	
Mean in group NOTPRIMED	4.257143	

The independent t-test showed that the mean in the group without priming intervention is 4.26 and the mean in the group with priming intervention is 5.0. Comparing the achieved p = 0.0008184 to the significance level of α=0.05, the independent t-test (F(34), t= -3.6726, p= 0.0008184) showed a statistical significant effect.

Hypothesis Two

Second, a t-test was conducted to compare whether there were age differences between younger and older participants in the selection of the QR codes upon receiving the priming intervention.

The survey found all the participants who had undergone priming intervention achieved perfect scores irrespective of age group. There was a ceiling effect, which meant that the priming intervention was so successful that age didn't have any effects. Hence the hypothesis is not supported.

Quantitative Analysis
Running the means analysis for QRtotal score, it shows the means is 1.69 with a standard deviation (sd) of 0.48 for the Age selected as shown in Table 6.

Table 7
Means Table

	mean	sd	skew	kurtosis
SURVEY	2.00	0.00	NaN	NaN
AGE	1.69	0.48	-0.73	-1.55
QRtotal	5.00	0.00	NaN	NaN

From Table 7, the distribution with a Skew of |0.73| and Kurtosis of |1.55|, was sufficiently normal for conducting a t-test. (which is within the scope of rule for Normality of Skewness <│2│ and Kurtosis <│9.0│).

There are no differences in the QR scores achieved by all the participants, young and old, who underwent primed intervention, hence there is no t-test conducted.

Discussion

Effectiveness of Priming Intervention

This study showed significant effectiveness (p <0.05) of priming intervention or a warning to prevent the choice of a QR code that leads to a "fictitious" or malicious website. Statistical analysis showed that priming invention influenced the degree of choosing the QR code that led to "authentic" website. However, it is also observed that even with the experiment group of no priming intervention, there is a sizeable number of participants who chose the QR code that led to "authentic" website. Although in the same experimental group of no priming intervention, that is where participants were observed to have chosen a QR code that leads to a “fictitious” or malicious website. Below, we discuss these results.

Priming & Warnings

This study showed that priming intervention is effective in alerting the participants in our survey in identifying the authentic QR codes. In the priming intervention condition, our participants were shown a warning poster before the start of the survey. Accordingly, they had to scan five sets of QR codes, and we noted that this controlled group had been alerted and had carefully scanned the QR code, pause and looked carefully at the URL presented. All the participants in this group had chosen only QR codes that led to “authentic” websites. Past research suggested that priming intervention on victimisation in cybercrime (Acquisti et al., 2012). To balance the views, it is also important to highlight other studies that do not support the effectiveness for priming intervention (Grazioli & Wang, 2001; Zhang & Xu, 2016) and another study that showed warnings was not effective, such as Hong (2012) which found that users did not find that browser warnings had positive effects. We expected that participants, when presented with a warning, before filling up the survey or questionnaire would prevent them from choosing the “fictitious” or malicious QR codes.

Effectiveness of Priming Intervention in Age Differences

Through the results of this study, it was found that there was no observable effect of age difference in the priming intervention group. Both groups, younger adults and older adults performed equally well, with all of them scoring perfect scores having undergone priming intervention. This has caused a ceiling effect which caused the priming intervention in age differences to have no effect.

Explanations for participants (without priming intervention) choosing a QR code that leads to a “fictitious” website.

No intervention

The first possible explanation is that without priming interventions or warnings, participants were not paying attention to the QR codes that they scanned and also did not observed the URL that the QR codes presented. Some were observed rushing through the survey.

Lack of knowledge

Without priming interventions or warnings provided, participants were not trained or provided with information, our observations during data collection suggest that many participants did not make the connection between the QR codes that was provided and the URL presented could be used for cybercrime or phishing. In support of this line of reasoning is the fact that, a sizable part of our respondents seemed to not realise that the QR codes scan had fictitious or malicious URL presented. They had assumed that all QR codes were valid and authentic.

Goal hierarchy

Participants might not give priority to security and their primary focus could be to complete the survey or chose answers for expediency. Our participants were doing this survey in an educational institution and in a classroom environment. They were “interrupted” to participate in a research and specifically, to fill out a survey. Given that their mind was focusing on their institutional environment, their favorable view of student led research surveys and completing their primary tasks, they could have filled it out without paying too much attention to security considerations.

Optimism bias

Generally, people tend to believe that negative events are less likely to happen to them than to others, and they believe that positive events are more likely to happen to them than to others

(Weinstein, 1980). Although this is a plausible line of reasoning, we did not see any indications of optimism bias in this study.

Distraction

People's attention at any single instance is limited. This has also been called 'selective attention'. In a situation for which participants had their classroom lessons interrupted or just completed their mid-term examination, to fill in a survey, they might have focused on going for a break or on going home respectively. This, in turn, may lead subjects to follow their 'default' option, which is obedience and less alert or aware in their selection of the QR codes and URL presented. We believe it is possible that this phenomenon explains the choices of QR codes leading to "fictitious" or malicious websites. It is interesting to note that to distract people is a common method used by attackers to defraud them (Stajano & Wilson, 2011).

Explanations for participants (without priming intervention) choosing a QR code that leads to an "authentic" website.

Technology Mastery

All the participants in this survey are students of part of the Master of Science in Security by Design (MSSD) in SUTD. The educational background and the technological savviness of the participants could explain why 24 of the 35 surveyed participants were about to get the select the QR codes that led to "authentic" website even though there were no priming intervention. Some of these participants could have already been aware of the dangers of QR codes and hence their confidence of using this QR code and technology.

Implications

Noteworthy, in the physical world, the effect of priming intervention had huge impact on the everyday tasks. We noted the use of priming intervention in television/movie/game content rating warnings for the suitability to the audiences such children, teenagers, or adults, to the acceptable use policy on the start-up screen for official computers employed in many organization's IT systems. From our survey result, it is also important that ample warnings be adopted by technology companies adopting QR codes to warn its users of what to look out for or to introduce some checks and warnings for the URL presented by scanning QR codes. It is also recommended that users adopt QR readers include the ability to check the authenticity and safety of destination websites.

Technology firms would also have the responsibilities to develop and adopt technologies that would make it difficult for QR codes to be spoofed. Recommended by Kevin et.al. (2014), one of the proposals was to embed digital signature information into the code to confirm its authenticity but uses more of the code's available space for the extra data. Another proposal was to use encryption to stop a third-party from snooping and cloning QR codes used for logging people in. To do this, the online app would send an encrypted QR code to an already logged-in (and therefore trusted) mobile device. Only the logged-in device can decrypt the QR code, which it then displays for the second device to read. The QR code contains a URL which logs them into the app.

Recommendation

We recommend priming intervention to be used to help increase awareness and influence users' actions. For example, in a poster where the police force would like to increase the public's awareness to deter online scamming, in addition to educating, the police force could consider including a question such as 'have you checked the URL?' and 'did you check if the link is authentic?'. Having such priming intervention would initiate the user to pause and think and is likely to influence the user's action.

Future Research

For future experiments, researchers should look at expanding this survey to include not only MSSD students or SUTD students, but a wider range of participants such as non-student groups and participants from the different age groups. The total number of survey participants could be increased and the timing it took to choose the correct QR codes could be recorded. This timing could be an indicator of whether the participants do take their time to check the URL presented. Thus, researchers can acquire more detailed records and could correlate the proportion of individuals that fell victim to such attacks and the time taken to check URL presented by scanning the QR codes. By expanding the survey outside the MSSD and SUTD, researchers could collect more information of the demographic of the people who do fall prey and observe which groups of individuals are more vulnerable. For the collected data to have any significance, more samples need to be collected.

Conclusion

QR codes are by no means a secure standard for data encoding in their current state. There is, however, great room for improvement.

QR codes have various advantages as an information sharing tool. They allow fast and easy distribution of various forms of structured data and have many applications in manufacturing and business. For QR codes to be used safely, users should be aware of the vulnerabilities inherent in the standard, in their particular reader, and the ease of social manipulation attacks. The key is having awareness of the various attacks presented in this paper and implementing preventative measures by use of the standards also presented. If this is done, QR codes can be used globally as an efficient standard for many different purposes.

New security standards mentioned by Kevin et.al. (2014) such as Symmetric Encrypted QR (SEQR) codes, Public Key Encrypted QR (PKEQR) codes, and Signed QR codes can be implemented within the existing QR standard. SEQRs allow for services such as login by scanning a QR code on a verified mobile device. PKEQRs would allow secure data to be distributed to a select group of people easily. SQRs allow users to check whether they trust the creators of QR codes before opening their potentially dangerous contents. All these methods come at some cost, either in space or time, and therefore should be used only when required, such as when using QR codes to share sensitive data within a company, and not in commercial use.

Despite the growing technology in QR codes to beef up security, it is still heavily dependent on the user’s knowledge and awareness to be able to identify an authentic from a fictitious QR code. This study found that priming intervention is effective. It was shown that a simple warning had effect on the participants’ choice.

In conclusion, priming intervention is effective to a huge extent and is recommended to increase users’ awareness to identify an authentic QR codes.

References

Caraban, A., Karapanos, E., Teixeira, V., Munson, S. A., & Campos, P. (2017). On the Design of Subly: Instilling Behavior Change During Web Surfing Through Subliminal Priming. *Persuasive Technology: Development and Implementation of Personalized Technologies to Change Attitudes and Behaviors Lecture Notes in Computer Science*, 163–174. doi: 10.1007/978-3-319-55134-0_13

Doyen, S., Klein, O., Pichon, C.-L., & Cleeremans, A. (2012). Behavioral Priming: Its All in the Mind, but Whose Mind? PLoS ONE, 7(1). doi: 10.1371/journal.pone.0029081

Grazioli, S., & Wang, A. (2001). Looking without seeing: Understanding unsophisticated consumers' success and failure to detect internet deception. In ICIS 2001 proceedings (p. 23).

Hong, J. (2012). The state of phishing attacks. Communications of the ACM, 55(1), 74e81. http://dx.doi.org/10.1145/2063176.2063197.

Junger, M., Montoya, L., & Overink, F.-J. (2017). Priming and warnings are not effective to prevent social engineering attacks. Computers in Human Behavior, 66, 75–87. doi: 10.1016/j.chb.2016.09.012

John, L. K., Acquisti, A., & Loewenstein, G. (2011). Strangers on a plane: Contextdependent willingness to divulge sensitive information. Journal of consumer research, 37(5), 858e873.

Kevin Peng, Harry Sanabria, Derek Wu, Charlotte Zhu (2014) Security Overview of QR Codes, 2014, MIT

Kieseberg, P., Leithner, M., Mulazzani, M., Munroe, L., Schrittwieser, S., Sinha, M., & Weippl, E. (2010). QR Code Security. *MoMM '10: Proceedings of the 8th International Conference on Advances in Mobile Computing and Multimedia*, 430–435. doi: 10.1145/1971519.1971593

Krombholz, K., Frühwirt, P., Kieseberg, P., Kapsalis, I., Huber, M., & Weippl, E. (2014). QR Code Security: A Survey of Attacks and Challenges for Usable Security. *Lecture Notes in Computer Science Human Aspects of Information Security, Privacy, and Trust*, 79–90. doi: 10.1007/978-3-319-07620-1_8

Krombholz, K., Fruhwirt, P., Rieder, T., Kapsalis, I., Ullrich, J., & Weippl, E. (2015). QR Code Security -- How Secure and Usable Apps Can Protect Users Against Malicious QR Codes. 2015 10th International Conference on Availability, Reliability and Security. doi: 10.1109/ares.2015.84

Mendelson, J., & Bergstrom, J. C. R. (2013). Age Differences in the Knowledge and Usage of QR Codes. Universal Access in Human-Computer Interaction. User and Context Diversity Lecture Notes in Computer Science, 156–161. doi: 10.1007/978-3-642-39191-0_18

Papies, E. K. (2016). Goal priming as a situated intervention tool. Current Opinion in Psychology, 12, 12–16. doi: 10.1016/j.copsyc.2016.04.008

Stein, R., Blanchard-Fields, F., & Hertzog, C. (2002). The Effects of Age-Stereotype Priming on the Memory Performance of Older adults. *Experimental Aging Research*, *28*(2), 169–181. doi: 10.1080/03610730252800184

Vidas, T., Owusu, E., Wang, S., Zeng, C., Cranor, L. F., & Christin, N. (2013). QRishing: The Susceptibility of Smartphone Users to QR Code Phishing Attacks. *Financial Cryptography and Data Security Lecture Notes in Computer Science*, 52–69. doi: 10.1007/978-3-642-41320-9_4

Weinstein, N. D. (1980). Unrealistic optimism about future life events. Journal of personality and social psychology, 39(5), 806.

Yong, K. S. C., Chiew, K. L., & Tan, C. L. (2019). A survey of the QR code phishing: the current attacks and countermeasures. 2019 7th International Conference on Smart Computing & Communications (ICSCC). doi: 10.1109/icscc.2019.8843688

Zhang, B., & Xu, H. (2016). Privacy nudges for mobile applications: Effects on the creepiness emotion and privacy attitudes. In Proceedings of the 19th ACM conference on computer-supported cooperative work & social computing. San Francisco: California, USA.

Appendix

Cyber crime research reproducibility checklist

4 April 2020

Good research leads to results that can be read *and* reproduced easily by others. To make your paper easy to read you should follow the APA guidelines, see http://www.apastyle.org

This short, 16-item checklist is intended to help you describe your research in sufficient detail for someone else to be able to repeat it, and thereby to refute or corroborate your findings.

Each answer should not be just a yes/no but be a short sentence. We provide some suggestions about a paper on a course evaluation in italic font below.

Please attach the checklist and your answers as an appendix to your own paper.

You will probably discover that while you are completing the checklist, you discover that your paper should be improved. Please do so before submitting the final version!

Abstract

1. Have you written the abstract with at least one sentence on the Background, Method and Results, and does it mention N?

Yes, the abstract has the IMRAD structure.

Background

2. Have you described the problem that led to your research?

Yes, we were interested in priming intervention influenced the choice of QR code (authentic from fictitious) of MSSD students.

3. Have you described the relevant background, and the key references from the peer reviewed literature in APA format on which your work is built?

Yes. 17 peer-reviewed papers are cited in APA format.

4. Have you listed a research question?

Yes. To what extent does priming intervention improve one's ability to distinguish "fictitious" from "authentic" Quick Response (QR) Code?

Method

5. Have you added a picture to summarise how the different groups are treated?

Yes, we have described the research design and illustrated it with a picture.

6. Have you described how you recruited your subjects and the number of participants?

Yes. Our subjects are the 51 students from SUTD MSSD course.

7. Have you described what you asked your subjects to do?

Yes, we asked our students to complete a survey (N=51).

8. Have you described how the control group was created, and how big it is? *Yes, the two groups were divided and chosen at random. We had no influence in the formation of groups.*

9. Have you described **all** the dependent and independent variables and how they are coded?
Yes.

Results
10. Have you described how you analysed your data?
Yes, we conducted t-test.

11. Have you described which statistical tests you applied to the data, and what the outcome of those tests is?
Yes, we conducted t-test.

Discussion
12. Have you summarised the background and purpose of your research?
Yes, we summarised the effect of priming intervention.

13. Have you described to what extent the research question has been answered?
Yes, we concluded that priming intervention is effective to a huge extent.

Limitations
14. Have you discussed the limitations of your research?
Yes.

Conclusions
15. Have you provided conclusions that reflect the key findings?
Yes, we summarise conclusions based on the statistically significant results.

16. Have you put your work in perspective as provided by the literature?
Yes.