A User Study of Security Warnings for Detecting QR Code Based Attacks on Android Phone

Dongwan Shin* and Huiping Yao
Secure Computing Laboratory
New Mexico Tech, Socorro, NM, USA
{doshin, hyao}@nmt.edu

Abstract

The security analysis of existing QR (Quick Response) code scanners on Android was conducted recently and the result shows that most of those QR code scanners were not able to detect attacks exploiting malicious URLs embedded in QR codes, especially phishing and malware attacks. In our previous study, we proposed a QR code scanner solution called *SafeQR* that utilized two well-known security APIs in order to improve the detection rate of those attacks. In this paper we discuss in detail a user study conducted to investigate the effectiveness of *SafeQR*, primarily from the perspective of user's security perception. Specifically, we first discuss how to design the security warnings of *SafeQR* using Microsoft's NEAT (Neat, Explained, Actionable, Tested) and SPRUCE (Source, Process, Risk, Unique, Choices and Evidence), and then we present how to design our user study to test their effectiveness. The result of our user study is promising, showing that *SafeQR* enables better user perception of imminent security threats, compared to other QR code scanners.

Keywords: QR code security, phishing, malware, visual warning, and user study

1 Introduction

Quick response code (QR code) has been popular due to its easy generation and distribution, large storage capacity, and fast readability [1]. According to a recent survey, 75% of retailers use QR codes to interact with and track potential buyers [2]. Generally, QR codes are used to direct users to the websites of their interest, which can provide further information or services. By scanning a QR code, however, users can be easily taken to a malicious website, for instance, a phishing website or one distributing malware. This is because users usually do not know the information encoded in the QR code until they scan it. Hence, attackers can exploit this and use QR codes for various types of attacks.

In this paper, we are mainly interested in phishing and malware attacks based on QR codes. Phishing attacks trick users to divulge their sensitive information by masquerading as a trustworthy entity [3, 4]. For instance, a QR code can redirect users to a fake bank website that looks exactly like the real bank website. A normal user will not be able to see the differences and thus type in her credential information that will be handed to the attackers [5, 6, 7]. On the other hand, a malicious QR code can also be used to redirect users to a URL distributing malware [8]. An early example of malware attacks through QR codes was that people were fooled into scanning a QR code and downloaded a malicious application, which sent off multiple text messages to a number that charged users $5 per SMS message [9]. There are other types of attacks such as social engineering [10, 5, 6, 9, 7] and cross-site attacks [11]. Though interesting, a complete study for these attacks is out of purview of this paper.

The security analysis of existing QR code scanners on Android was conducted recently and the result shows that most of those QR code scanners were unable to detect attacks exploiting malicious

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, volume: 4, number: 4, pp. 49-64
*Corresponding author:Computer Science Department New Mexico Tech, Socorro, NM 87801, USA, Tel: 1-575-835-6459

URLs embedded in QR codes, especially phishing and malware attacks [12]. In the study, 31 QR code scanners available at the Google Play were analyzed in terms of their security features and security warning capabilities, and two top-rated QR code scanners, Norton Snap and QR Pal, were selected and tested against phishing attacks exploiting malicious URLs embedded in QR codes. The test results ware quite alarming with Norton Snap being able to detect only 28.0% (112/400, 95% Confidence, CI-4.25%) of phishing URLs and QR Pal only 27.75% (111/400, 95% Confidence, CI-4.24%).

In our previous study, a secure QR code scanner solution called *SafeQR* was proposed to better detect phishing and malware attacks based on malicious embedded URLs [12]. *SafeQR* utilized two well-known security APIs, Google Safe Browsing API and Phishtank API, in order to improve the detection rate for the attacks. In this companion paper, we discuss in detail the design of a user study to test a set of hypotheses on user awareness of QR code based threats, effectiveness of QR code based attacks, helpfulness of visuals security warnings, and habituation effect. Specifically, we first discuss how we designed the security warnings of *SafeQR* using Microsoft's (Neat, Explained, Actionable, Tested) and SPRUCE (Source, Process, Risk, Unique, Choices and Evidence), and then how we designed and conducted our user study to test their effectiveness. The result of our user study is promising, showing that *SafeQR* enables better user perception of imminent security threats, compared to other QR code scanners.

The rest of the paper is organized as follows: Section 2 briefly discusses our QR code scanner solution. Section 3 discusses the methodology and design of a user study developed to test the effectiveness of our approach. Section 4 and 5 present and discuss the results of the user study. Section 6 concludes the paper.

2 Design of *SafeQR*

The design of *SafeQR* was motivated by the poor detection performance of existing QR code scanners. Hence our design approach aimed at achieving two goals for *SafeQR*; the first was to enhance the effectiveness of detecting malicious URLs used for phishing and malware attacks, while the second was to improve user perception of security when a QR code is scanned and used so that users can make a better security decision.

2.1 Design for Better Detection

Two well-known security APIs, Google Safe Browsing API [13] and PhishTank API [14], were adopted for our solution to improve the effectiveness of detecting malicious URLs. Safe Browsing, developed by Google, is a service that enables applications to check URLs against Google's constantly updated lists of suspected phishing and malware websites. For simplicity, we chose Safe Browsing Lookup API [15], queried the URLs through HTTP GET request, and got the state of the URL(s) directly. PhishTank contains a blacklist of phishing URLs consisting of manually verified websites. PhishTank provides API for developers to lookup a URL's status in their database. We used the API to query a URL's status, thus further enhancing the capability for detecting phishing scams.

Additionally, if the URL string ends with .apk (the Android application package file extension), we assume that a non-official Android market application will be downloaded to a user's mobile phone when the URL is scanned and visited. If the "Unknown Sources" setting is checked in Android, the application will be automatically downloaded to the user's Android device. A dialog will pop up otherwise to ask the user if she wants to check the option to download the app. Users can easily tick the "Unknown Sources" option just by following the instructions in the pop-up dialog, and then download and install the application. Our solution checks if the URL ends with ".apk", and if it does, then we provide potential warnings to users, as shown in Figure 1.

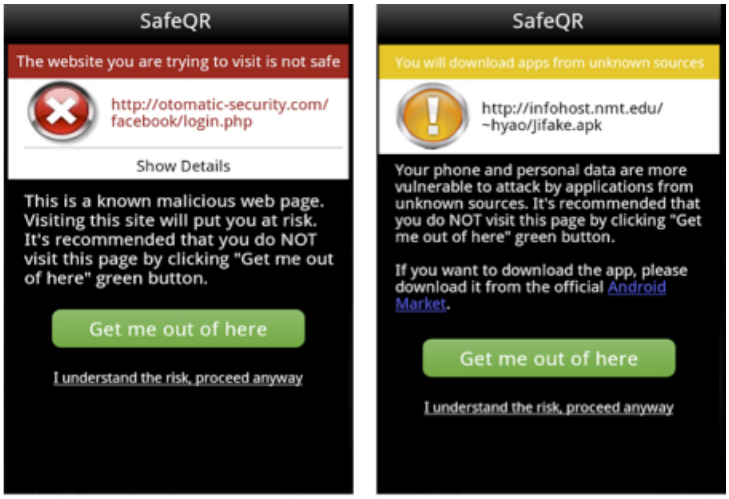

Figure 1: Our UI Design: (left) When detecting a phishing or malware URL; (right) When detecting an URL ending with ".apk"

Algorithm 1: Detection

```
Data: url - an input URL that is to be evaluated
Result: status - an evaluation result
status = 0;                                                    // a safe URL
if GoogleSafeBrowsingCode(url)==200 then
    if containsPhishing && containsMalware then
        status = 3;                                // a both malware and phishing URL
    else if containsMalware then
        status = 2;                                                // a malware URL
    else if containsPhishing then
        status = 1;                                               // a phishing URL
end
if InPhishtankList(url) then
    if status==0 || status==2 then
        status++;
    end
end
if status==0 && endWithAPK(url) then
    status = 4;                                  // a safe URL but ends with ''.apk''
end
```

The detection algorithm for our solution is outlined in the following pseudo code. The status variable in the code represents the security status of a URL, which has five different values. The status variable is initialized to 0, implying a safe URL. Its value becomes 1 when a URL is detected as a phishing one, 2 when a URL is detected as a malware website, 3 when a URL is a both phishing and malware site, 4 when a URL is checked safe through the Safe Browsing and PhishTank but ends with ".apk".

2.2 Design for Better Perception

Previous studies have shown that warning designs affect user's decision to obey or ignore the warnings [16, 17]. Therefore, designing an effective security warning by providing better risk perception was a significant part of our solution. We decided to apply existing warning design recommendations [16, 18] and Microsoft's NEAT (Neat, Explained, Actionable, Tested) and SPRUCE (Source, Process, Risk, Unique, Choices and Evidence) [19] into our warning message design as follows: we first set the warnings mainly with black and red colors, since this color combination is very effective to prevent users from attacks [16]; we made the safest button "Get me out of here", as a recommended action, most visible by setting its background green, which also helps users think of safe actions; since users are likely to ignore lengthy text, we only include necessary words for the warning, giving users a chance to click "Show Details" button for viewing details. In addition, only simple words are used, for users will not understand or will misinterpret technical jargons.

Two screenshots of our solutions are captured in Figure 1. The left screenshot shows the display of our solution when a user scans a QR code with a phishing or malware URL. On the other hand, the right sceenshot is the display when a user scans a QR code whose encoded URL ends with ".apk". If the website addressed by the URL is a phishing website or one containing malware, we immediately return a negative evaluation, which is shown in Figure 1. If the URL ends with ".apk", we return an uncertain evaluation for .apk file may be not a malware.

3 User Study

We conducted a user study not only to explore the effectiveness of the security warning of *SafeQR* but also to compare it against those of two existing solutions, namely the security warnings provided by Norton Snap and QR Pal[1], as shown in Figure 2. We also wanted to study how all of these solutions compare against the absence of any visual security warning. Finally, we wanted to test all of the security warnings in the presence of QR code based phishing attacks.

To test different scenarios that will be elaborated later, we devised four different user groups, each of which is exposed to a different kind of warnings or no warning at all. Specifically, 3 different user groups were exposed to Norton Snap, QR Pal, and our solution *SafeQR* respectively, the remaining user group was exposed to QR code Scanner, which has only a user confirmation feature but no warning message[2].

To avoid the framing effect, we did not want the users to be aware that we were testing their reaction to a security warning. In addition, we wanted the users to be exposed to the warnings as an abnormality or exceptional condition. To achieve both goals, we told the participants that we were investigating whether they made full use of smart phone apps, and evaluating the usability of using QR code scanners to access websites. The participants were given an Android smart phone where the QR code apps were installed and were told that we would be interested in improving the usability of the apps, so they were encouraged to use the app with their real credentials to help us achieve the goal. Users were assigned randomly to one of the user groups and given the same instruction. After they scanned a QR code, a security warning would be displayed. It was what the participants decided to do at this point that we were interested in. Since we did not want to expose the users to any real danger (or violate our university's IRB policy), we prevented an actual login from occurring on the smart phone and redirected the participants to the exit survey instead.

Before conducting our user study, we defined a set of hypotheses we wanted to have tested. The hypotheses we developed are as below:

[1]Note that we conducted a thorough analysis on the security and warning features of Norton Snap and QR Pal along with our solution so readers interested in the analysis should refer to our earlier study [12].

[2]Again please refer to our earlier study on these features at [12].

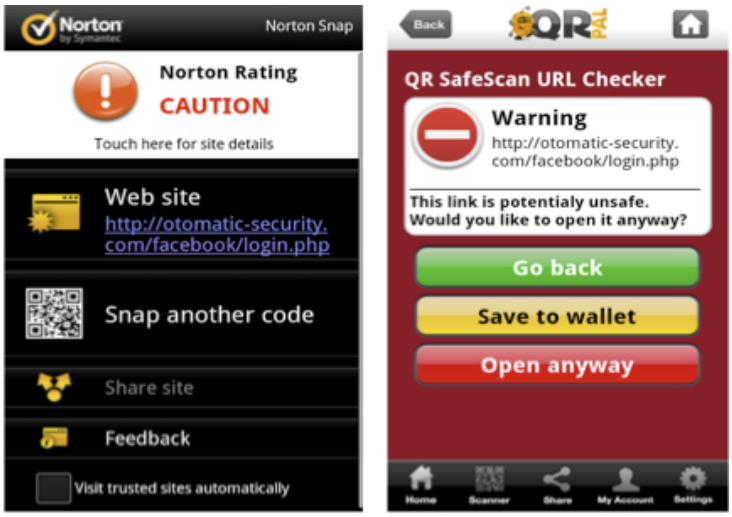

Figure 2: Warning messages displayed in two existing QR code scanners: (lett) Norton Snap; (right) QR Pal

1. (*Unawareness of malicious QR codes*) Users will not realize security problems in QR codes.
2. (*Effectiveness of QR code based phishing attacks*) Users tend to submit their credentials after scanning with QR code scanners without security warnings.
3. (*Helpfulness of security warnings*) Users will not open the URL, when warned with security warning messages. Even if users open the website, they tend not to submit their credentials.
4. (*Better effectiveness of our warning design*) More users tend to not open the link or submit their credentials in the presence of our warning design.
5. (*Habituation effect*) Previous experience of exposure to similar warnings affects user's behavior.

The first hypothesis assumes that the average users are not aware of malicious QR codes. Given this knowledge, the second hypothesis tests whether users are able to identify QR code based phishing attack, meaning that most users are unable to identify phishing URLs when scanning the QR codes. The third hypothesis tests the assumption that security warnings do help users detect malicious attacks. The fourth hypothesis is related to our proposed solution. We hypothesized that our security warning is more effective than existing ones. The last hypothesis is related to the habituation effect, and we hypothesized that habituation will affect user behaviors even if they notice and understand the warning message.

3.1 Experimental Design

We defined four separate user groups, each of which was exposed to a different warning provided by a different QR code scanner.

- Group 1: Exposed to the attack with no warning, using QR code Scanner
- Group 2: Exposed to the attack with Norton Snap's warning
- Group 3: Exposed to the attack with QR Pal's warning
- Group 4: Exposed to the attack with our designed warning

(a) Black white QR code (b) QR code with color

(c) QR code with Facebook logo (d) QR code with both Facebook logo and color

Figure 3: Four different types of QR codes

Users were assigned randomly to one of those user groups and given instructions. The instruction sets were identical for all the users. At first, we asked users to finish a pre-survey to investigate how much users know about QR codes. Then, users were instructed to choose one of the four different types of QR code (i.e. black white QR code, QR code with Facebook logo color, QR code with Facebook logo, QR code with both Facebook logo and color), shown in Figure 3, and scan it to visit our survey website on Facebook. Users needed to login using their credentials and to fill out our survey online. After that, participants were told to answer a brief exit survey that includes questions on the overall understanding of security warnings and its consequences.

Each participant was exposed to only one scenario in the study. Users were asked to act as if they were using their own phone, in that all decisions they made should be the same as if they were being made on their own private phone. Security was never explicitly mentioned. To avoid making users aware of our real purpose, the experiment script was carefully designed so that the users thought they were being tested on the usability of QR code and QR code scanners to access websites and not on the security of QR code.

3.2 Sample

In the design of our experiment, we performed a power analysis to determine the minimum sample size that we would require to test our hypotheses. We chose an error of 0.05 and a power of 0.8, common among such experiments, and determined a minimum sample size of 19 subjects across the four user groups. In our study, volunteers were elicited by posted fliers around our campus and offering an iPod Touch as a prize to be drawn among the participants. A total of 87 individuals replied to our request, from which 5 did not have a Facebook account and 2 did not finish the survey form, which were discarded. A total of 80 valid submissions were obtained, 20 individuals per group, therefore above our minimum sample size and enough to test our hypotheses. The subjects who participated in our study mostly came from our university. The demographic details will be presented in the beginning of Section 5.

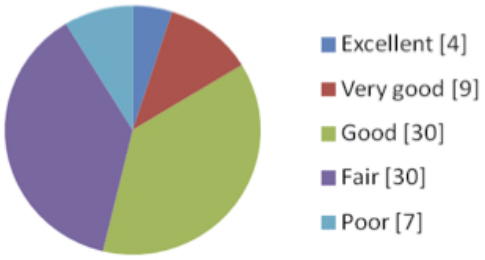

Figure 4: Distribution of security knowledge

3.3 Exit Survey

The last step asked to the participants of our study was to answer a brief exit survey that included questions on the overall understanding of the presence of warnings in QR code scanners and the user's opinions on the different warning mechanisms. The users were asked to specify whether they noticed, read, and understood the warnings. Users were also asked to quantify their concern with the security of their credential submission to a website. Finally, the users were asked to answer a few questions on their own information, such as gender, education, major, level of security knowledge.

4 User Study Results

Our sample includes 80 individuals, who participated in our study on campus. There were 20 female and 60 male participants. Our participants have a high education rate, with all having completed at least high school degree, and 83.75% (67/80) having or currently pursuing undergraduate college degrees. Age groups of our participants include 38 from 10-20 years old, 32 from 21-30 years old, 5 from 31-40 years old, 2 from 41-50 years old, 2 from 51-60 years old, 1 from 61-70 years old. Relative to security knowledge, the participants are very sophisticated, with only 7 claiming they have poor security knowledge. As shown in Figure 4, 54% (43/80) of the participants replied that they had good security knowledge or above.

4.1 Hypothesis 1: Unawareness of Malicious QR Codes

The hypothesis was tested by asking all the users whether they had ever thought of any security problem in QR codes in the exit survey. Out of 80 subjects, 67.5% (54/80, CI: 56.6% - 76.8% with 95% confidence) were not aware that malicious QR codes existed. The statistical test result (z-statistic = 3.130, P = .0017) allows us to conclude that the test result was statistically significant. Hence, we conclude that most of the users are unaware of malicious QR codes.

4.2 Hypothesis 2: Effectiveness of QR Code Based Phishing Attacks

On our second hypothesis, we assume that phishing attacks based on QR codes are effective when a user visits a website and submit her credential after scanning a QR code using her QR code scanner. To test this hypothesis, we had the first group of users exposed to phishing attacks and not shown any warning. We postulate that the average user will not perceive this attack situation. However, there is still the possibility that a savvy user would be able to detect the attack by inspecting the URL and thus not visiting the website. The summary of test results is shown in Table 1.

Table 1: Effectiveness of QR code based phishing attacks

Action	Count	95% CI
Open	20 (out of 20)	0.838 - 1.000
Submit	15 (out of 20)	0.531 - 0.889

As it can be seen from Table 1, of the twenty users in the first user group, 100% (20/20) opened the link and 75% (15/20) submitted their Facebook username and password. Among the remaining five participants, only one pointed out the specific reason that the web address of the link was suspicious, while the other four replied that they felt unsafe for some reasons. Based on the test results (z-statistic=2.236, P=.0253), we conclude that without any added security mechanisms in QR code scanners, QR code based phishing attack will be highly effective against the average user.

4.3 Hypothesis 3: Helpfulness of Security Warnings

Since most users were not aware of malicious QR codes, our third hypothesis was to evaluate whether security warnings provided by the QR code scanners effectively prevent users from attacks. This means that the average people will notice the warnings, thus not submitting their credentials. To test this hypothesis, we had the three groups except the first group exposed to the warnings. The results of our experiments are summarized in Table 2.

Table 2: Open and submit actions for the four different study groups

	Open	Submit
QR code Scanner	20	15
Norton Snap	15	7
QR Pal	9	7
SafeQR	3	2

We compared the three QR code scanners with security warning, Norton Snap, QR Pal, and *SafeQR*, against QR code Scanner which does not provide security warning respectively in terms of both open and submit actions. The summary of the statistical significance of the difference between different groups is shown in Table 3 - 8.

Table 3: Comparison of open action between Norton Snap and QR code Scanner

	Open	Not Open	Fisher's Exact P
QR code Scanner	20	0	0.047
Norton Snap	15	5	

We can see from Table 3 that 15 out of the 20 users in Norton Snap group opened the website, while 5 refused to open. Table 4 shows 7 out of 20 submitted their credentials, while 13 refused to continue. The statistical test results show that they are statistically significant. Hence, we reject the null hypothesis that QR code Scanner and Norton Snap are equally helpful to prevent users from submitting their credential to the phishing website. From Table 5, only 9 out of the 20 users opened the website, while 11 chose not to open. From Table 6, 7 out of the 20 users submitted their credentials, while 13 refused the submission.

Table 4: Comparison of submit action between Norton Snap and QR code Scanner

	Submit	Not Submit	Fisher's Exact P
QR code Scanner	15	5	0.025
Norton Snap	7	13	

Table 5: Comparison of open action between QR Pal and QR code Scanner

	Open	Not Open	Fisher's Exact P
QR code Scanner	20	0	0.000
QR Pal	9	11	

Table 6: Comparison of submit action between QR Pal and QR code Scanner

	Submit	Not Submit	Fisher's Exact P
QR code Scanner	15	5	0.025
QR Pal	7	13	

Similar to the previous test case, the statistical test results show that QR code Scanner and QR Pal are not equally helpful.

Table 7: Comparison of open action between SafeQR and QR code Scanner

	Open	Not Open	Fisher's Exact P
QR code Scanner	20	0	0.000
SafeQR	3	17	

Table 8: Comparison of submit action between SafeQR and QR code Scanner

	Submit	Not Submit	Fisher's Exact P
QR code Scanner	15	5	0.000
SafeQR	2	18	

Similar to the previous two test cases, the statistical test results show that our solution is different from QR code Scanner in terms of its helpfulness, as shown in Table 7 and 8.

From the analysis of Table 3 - 8, we can conclude that there is evidence to support that visual warnings do help users better perceive imminent threats from malicious URLs and act accordingly.

There was an interesting phenomenon that some users did not submit their credentials after opening the website. Specifically, in Norton Snap user group, 8 out of 15 users who opened the sites chose not to submit their credentials. In QR Pal user group, only 2 out of the 9 users did not submit their credentials. In *SafeQR* user group, only 1 user out of 3 did not submit his credential after opening the website. The main reason behind this seems to be that they were just curious to see where they were taken to. Interestingly, we find that Norton Snap group has a significant difference from the other two groups. And the reason behind this seems to be related to the fact that 4 out of the 8 users in Norton Snap group did not notice or understand the Norton's warning message.

4.4 Hypothesis 4: Better Effectiveness of Our Warning Design

The main goal of our user study was to investigate the effectiveness of our designed warnings to clearly inform the users of a threatening situation. Specifically, we tested if our warning design is better than Norton Snap and QR Pal by using Wogalter's Communication-Human Information Processing (C-HIP) model [19], which provides a framework to identify whether a warning is effective or not. We asked the following questions to examine the different steps in Wogalter's model:

1. Attention switch and maintenance. Do users notice and read the warnings before they proceed?
2. Comprehension and memory. Do users know what the warning message mean? Do users know what they are supposed to do when they see the warning message?
3. Attitudes and belief. Do users believe the warning?
4. Motivation and behavior. Are users motivated to take the recommended actions? Will users actually perform those actions?

4.4.1 Attention Switch and Maintenance

The first stage in the C-HIP model is "attention switch", meaning good warning designs are able to catch the user's attention and cause attention maintenance. Specifically, we asked users in our exit survey whether they had noticed the warnings and whether they had read the warnings completely.

Table 9 shows 85% (17/20) of Norton Snap users noticed the warning, with 55% reading it completely; 95% (19/20) of QR Pal users noticed the warning, with 90% reading it; 100% (20/20) of *SafeQR* users noticed our security warning, with 90% (18/20) reading it completely. These results show that, in terms of attention switch and maintenance, our solution has a significant advantage over Norton Snap, and that our warning design is as effective as QP Pal.

Table 9: For different groups, # of warning notice and read

	Norton Snap	QR Pal	SafeQR
Notice warning	17	19	20
Read warning	11	18	18

4.4.2 Warning Comprehension

A well-designed warning conveys the danger clearly and commends users the safer option. In the exit survey, we asked participants whether they understood what the security warning wanted them to do.

Table 10: For different groups, # of warning comprehension

	Norton Snap	QR Pal	SafeQR
Understand warning	11	19	20

As seen in Table 10, the results show that only 11 out of the 20 users apprehended what Norton Snap wants to convey, 19 out of the 20 users understood QR Pal's warning message, 20 out of the 20 users understood the warning provided by our solution *SafeQR*. Though Table 12 shows that there is no significant difference between QR Pal and our solution, Table 11 shows a significant difference between

Table 11: Comparison of Norton Snap and SafeQR

	Understand	Not understand	Fisher's Exact P
Norton Snap	11	9	0.001
SafeQR	20	0	

Table 12: Comparison of QR Pal and SafeQR

	Understand	Not understand	Fisher's Exact P
QR Pal	19	1	1.000
SafeQR	20	0	

our solution and Norton Snap. The overall results showed that our solution conveys the warning and the recommended action clearly, thus more users understand our warnings.

4.4.3 Attitudes and Beliefs

To test "attitudes and beliefs" in C-HIP model, participants were asked to classify them in a given five-point Likert scale (1=Very low up to 5=Very high) for the question that to what degree they trusted the warning. The results are shown in Figure 5.

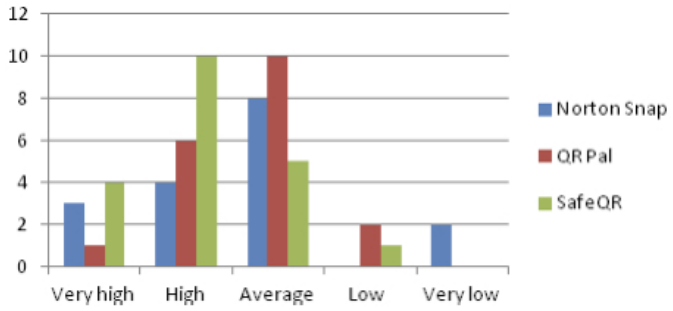

Figure 5: Comparison of user trust degrees for different groups

The results show that our warning design gains higher trust of the warning than the other two QR code scanners. 35% (7/20) of the participants trusted Norton Snap or QR Pal high or very high, 70% (14/20) of participants trusted our warning high or very high. In terms of attitudes and beliefs, our warning is significantly effective when compared to Norton Snap and QR Pal.

4.4.4 Motivation and Warning Behaviors

As one of the most important stages, users were asked whether they opened the link in the presence of warning messages, and whether they submitted their Facebook usernames and passwords. The statistical results were calculated in Table 13 - 16 according to the raw data in Table 2.

The statistical test results in Table 13 and Table 14 show that they are statistically significant. Hence, we reject the null hypothesis that Norton Snap and *SafeQR* are equally helpful to prevent users from submitting their credential to the phishing website. Similarly, the statistical results in Table 15 and Table 16 show that our novel design gains significant difference from QR Pal, in the terms of motivation and warning behaviors in the C-HIP model.

Table 13: Comparison of open action between Norton Snap and SafeQR

	Open	Not Open	Fisher's Exact P
Norton Snap	15	5	0.000
SafeQR	3	17	

Table 14: Comparison of submit action between Norton Snap and SafeQR

	Submit	Not Submit	Fisher's Exact P
Norton Snap	7	13	0.127
SafeQR	2	18	

Table 15: Comparison of open action between QR Pal and SafeQR

	Open	Not Open	Fisher's Exact P
QR Pal	9	11	0.082
SafeQR	3	17	

Table 16: Comparison of submit action between QR Pal and SafeQR

	Submit	Not Submit	Fisher's Exact P
QR Pal	7	13	0.127
SafeQR	2	18	

4.5 Hypothesis 5: Habituation Effect

Our last hypothesis stated that if users have become habituated to seeing similar-looking warnings when browsing legitimate websites, they are likely to ignore similarly-designed warnings regardless of the danger they present. To test this hypothesis, we asked participants to write down the reason why they opened the link even after they saw security warnings. The results showed that only two subjects mentioned they always opened the sites for the security warnings may have errors. The sample was not big enough to support the hypothesis.

5 Other Results and Discussion

5.1 Usage and Internet of QR Codes

Since the popularity and usage of QR codes are relevant to the topic of this research, we include in the presurvey questions related to them. It was interesting to find that only 67.5% (54/80) of the subjects knew what QR codes were, while all the subjects claimed that they saw a QR code at least once before. We also asked where the participants had seen a QR code and whether they had ever scanned one, and the result turned out similar to the survey result conducted by MGH [20]. As to the question of what they used a QR code for, the answers, shown in Figure 6, showed that the most common reason for the participant in our study to scan QR codes is to access additional information.

Among 80 participants, 66 owned a smart phone. 54.5% (36/66) of them installed one or more QR code scanners in their phones. We also asked how often they scanned QR codes [21]. Their response is summarized in Figure 7.

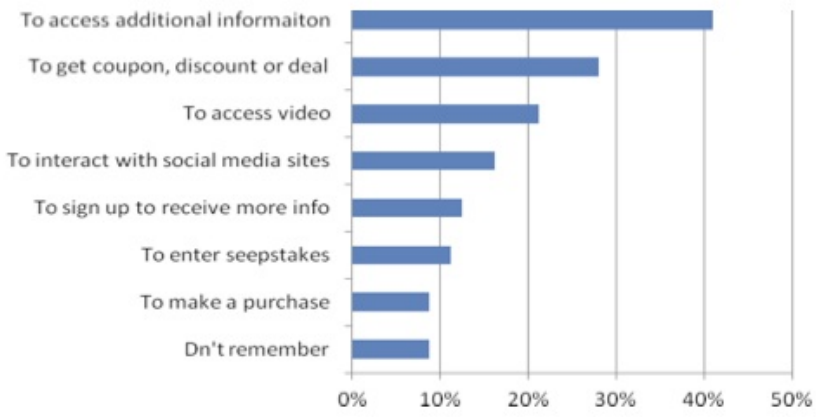

Figure 6: Distribution of reasons why users scan QR codes

Figure 7: Distribution of how often users scan QR codes

Additionally, it was interesting to figure out why users did not always scan QR codes, and we summarize the reasons as follows: 1) no internet; 2) no time; 3) no interest; 4) laziness; 5) security; 6) lack of knowledge about QR codes. The distribution is shown in Figure 8.

Note that out of 36 users who specified the reasons why they did not always scan QR codes, only 8% (3/36) chose security as their main reason for that.

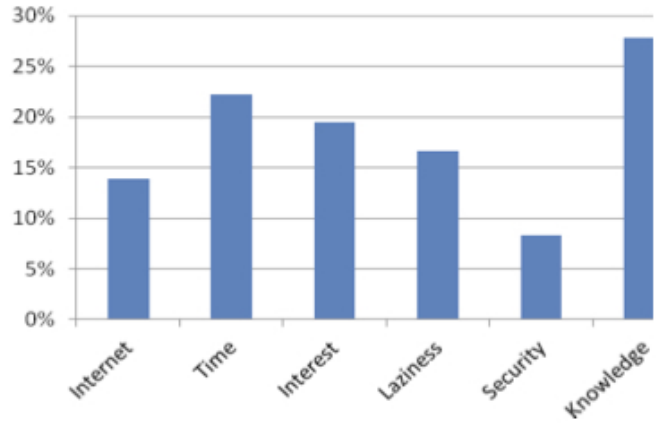

Figure 8: Distribution of reasons why users do not always scan QR codes

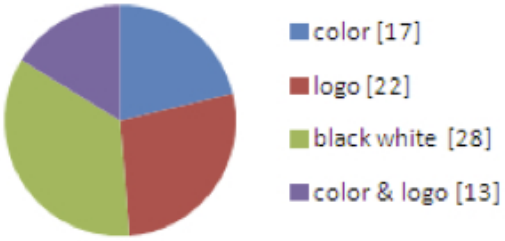

Figure 9: Distribution of user choice of QR code types

We also provided the participants four optional QR code types as follows: black white QR code, QR code with Facebook logo color, QR code with Facebook logo, and QR code with both Facebook logo and color. During the survey, we asked the users to choose one type they wanted to scan. The summary of their response is shown in Figure 9.

Most people chose black white QR codes, since it looked simple, familiar and traditional. Users who scanned colored QR codes said they simply liked the blue color and thought it appealing. Users who scanned QR code with Facebook logo reasoned as below:

- "The color contrast was nice"
- "It's more eye catching and appealing to look at and it told me what it was for"
- "The Facebook logo led credibility"
- "It said Facebook on it"
- "Guaranteed and security"
- "I could know what this QR used for"

The reasons for choosing QR code with Facebook logo can be summarized to two aspects: attractiveness and credibility. On the other hand, this also means that it seems easier to trick users by adding a famous logo inside of a QR code.

5.2 Usage and Knowledge of Android Phones

In the presurvey, we also asked the usage and knowledge of Android phones. 40.0% (32/80) of the participants used Android phones. 70% (28/32) of the Androiders had a good knowledge of, when asked, whether they knew that Android apps could be downloaded from other websites than Google Play store. However, only 50% (16/32) of the Androiders actually downloaded apps from other websites than Google Play store. Some Androiders who only downloaded apps from Google Play reasoned that Google apps were satisfactory, and they did not find anything interesting at the third party markets. Only 18.75% (3/16) participants chose as their main problem security such like viruses, and they did not trust the third party markets.

The above statistics show that most users had a good knowledge about installing apps from non-official sources on Android. However, most users seem not aware that they would be more vulnerable to malware if apps were downloaded and installed from non-official Android markets.

6 Conclusion

In this paper, we discussed in detail a user study to test the effectiveness of a secure QR code scanner called *SafeQR*. The result of our user study shows that a majority of users are not aware of QR code based attacks, that QR code based phishing attacks are quite effective, and visual security warnings are very useful for users to perceive imminent phishing attacks exploiting malicious URLs embedded in QR codes.

This research is by no means complete. Our user study used a sample consisting mainly of higher education students, a demographic that does not represent the average users accurately. We will investigate how to gather more representative samples. Additionally, due to the sample size, our habituation test was not completed. We will study how to address this important issue in our next round of user study.

Acknowledgement

This work was partially supported at the Secure Computing Laboratory at New Mexico Tech by the grant from the National Science Foundation (NSF-IIS-0916875).

References

[1] C. W. Bong, H. K. il, L. W. Gyu, P. W. Hyung, , and C. T. Myoung, "The New Vulnerability of Service Set Identifier (SSID) Using QR Code in Android Phone," in *Proc. of the 2011 International Conference on Information Science and Applications (ICISA'11), Washington DC, USA*. IEEE, April 2011, pp. 1–6.

[2] CNET, "The Dark Side of QR Codes," 2012. [Online]. Available: http://news.cnet.com/8301-1009_3-57464276-83/the-dark-side-of-qr-codes/

[3] R. Dhamija, J. D. Tygar, and M. Hearst, "Why Phishing Works," in *Proc. of the 2006 Conference on Human Factors in Computing Systems (ACM SIGCHI'06), Montréal, Québec, Canada*. ACM, May 2006, pp. 581–590.

[4] P. Soni, S. Firake, and B. B. Meshram, "A Phishing Analysis of Web based Systems," in *Proc. of the 2011 International Conference on Communication, Computing Security (ICCCS'11), Rourkela, Odisha, India*. ACM, February 2011, pp. 527–530.

[5] A. P. Felt and D. Wagner, "Phishing on mobile devices," in *Proc. of the IEEE 2012 Symposium on security and Privacy (IEEE S&P'12), Oakland, California, USA*. IEEE, May 2012.

[6] P. Kieseberg, M. Leithner, M. Mulazzani, L. Munroe, S. Schrittwieser, M. Sinha, and E. Weippl, "QR Code Security," in *Proc. of the 8th International Conference on Advances in Mobile Computing & Multimedia (MoMM'10), Paris, France*. ACM, November 2010, pp. 430–435.

[7] V. Sharma, "A Study of Malicious QR Codes," *International Journal of Computational Intelligence and Information Security (IJCIIS)*, vol. 3, no. 5, pp. 12–17, May 2012.

[8] Z. Yajin and J. Xuxian, "Dissecting Android Malware: Characterization and Evolution," in *Proc. of the 2013 IEEE Symposium on Security and Privacy (IEEE S&P'13), Oakland, California, USA*. IEEE, May 2012, pp. 95–109.

[9] Securelist, "Monthly Malware Statistics: September 2011." [Online]. Available: www.securelist.com/en/analysis/204792195/Monthly_Malware_Statistics_September_2011

[10] L. Borrett, "Beware of Malicious QR Codes." [Online]. Available: http://www.abc.net.au/technology/articles/2011/06/08/3238443.htm

[11] A. Kieyzun, P. J. Guo, K. Jayaraman, and M. D. Ernst, "Automatic Creation of SQL Injection and Cross-site Scripting Attacks," in *Proc. of the 31st International Conference on Software Engineering (ICSE'09), Vancouver, British Columbia, Canada*. ACM and IEEE, May 2009, pp. 199–209.

[12] H. Yao and D. Shin, "Towards Preventing QR Code Based Attacks on Android Phone using Security Warnings," in *Proc. of the 8th ACM Symposium on Information, Computer and Communications Security (ASIACCS'13), Hangzhou, China*. ACM, May 2013, pp. 341–346.

[13] Google, "Safe Browsing API." [Online]. Available: https://developers.google.com/safe-browsing

[14] PhishTank, "OpenDNS. PhishTank API Information." [Online]. Available: http://www.phishtank.com/api_info.php

[15] Google, "Safe Browsing Lookup API Developer's Guide." [Online]. Available: https://developers.google.com/safe-browsing/lookup_guide

[16] J. Sunshine, S. Egelman, H. Almuhimedi, N. Atri, and L. F. Cranor, "Crying Wolf: an Empirical Study of SSL Warning Effectiveness," in *Proc. of the 2009 Conference on USENIX Security Symposium, Montreal, Canada*. USENIX, August 2009, pp. 399–416.

[17] S. Egelman, L. F. Cranor, and J. Hong, "You've Been Warned: an Empirical Study of the Effectiveness of Web Browser Phishing Warnings," in *Proc. of the 2011 ACM Conference on Human Factors in Computing Systems (CHI'08), Florence, Italy*. ACM, April 2008, pp. 1065–1074.

[18] L. Zeltser, "How to design security warnings to protect users." [Online]. Available: http://blog.zeltser.com/post/3638747689/designing-security-warnings

[19] R. Reeder, E. C. Kowalczyk, and A. Shostack, "Helping Engineers Design NEAT Security Warnings," in *Proc. of the 2011 ACM Symposium On Usable Privacy and Security (SOUPS'11), Pittsburgh, PA, USA*. ACM, June 2011.

[20] MGH, "MGH's QR Code Usage and Inertest Survey," 2011. [Online]. Available: http://mghus.com/assets/managed/QR%20code%20Stats%203%2023%2011.pdf

[21] Forbes, "Are QR Codes Dead?" 2012. [Online]. Available: http://www.forbes.com/sites/ilyapozin/2012/03/08/are-qr-codes-dead

---

Author Biography

Dongwan Shin is an Associate Professor in the Computer Science and Engineering Department at New Mexico Tech. His research focuses on information and system security. He is the founding director of the Secure Computing Laboratory and faculty researcher at the Institute of Complex Additive Systems Analysis (ICASA) at New Mexico Tech. His research at Tech has been supported by NSF, DoD, Sandia Labs, Los Alamos Lab, Intel, VirtualBridge, and CAaNES. Dr. Shin received his Ph.D. in Information Technology from the University of North Carolina at Charlotte in 2004.

Huiping Yao is currently a doctoral student in the Computer Science and Engineering Department at New Mexico Tech, working as research assistant at Secure Computing Laboratory. She received her B.S. in Computer Science and M.S. in Computer Application Technology from Soochow University, Suzhou, China, in 2007 and 2010, respectively. Her research focuses on information security and privacy.