RESEARCH NOTE ON
QR CODES AND INFORMATION PROTECTION

Jing Yang, MMI, School of Business and Economics, State University of New York at Oneonta, Oneonta, NY, 13820, 607-436-3381, jing.yang@oneonta.edu

ABSTRACT

The development of internet and telecommunication urges researchers to look for a better way to secure end-users' private information. This study is rooted in end-user account protection, measuring the effect of QR codes on fear appeals and information protection. This study contributes to the extant literature by integrating two theories – protection motivation theory and the theory of planned behavior, as well as measuring an emerging technique in term of information security. The main goal of this study is to investigate how the co-use of computers and mobile devices can better protect end-users' privacy.

INTRODUCTION

The development of IT is gradually changing our lives. Reports show that since 1999 the number of internet users has increased tenfold and reaches around 40% of the word population in 2014[1]. Besides, more than half of the U.S. populations nowadays own a smartphone and spend an average of two hours per day on their mobile devices[2]. Many of our daily activities (for example, online banks, online shopping, and online social networks and so on) are accomplished in a virtual approach with the aid of internet and mobile devices. A concept regarding this virtuality is called Augmented Reality (AR). Technically, AR describes a live view of real world environment whose elements are merged with augmented computer-generated images (i.e. live-video, 2D images, or 3D virtual objects, etc.) to create a mixed reality [1]. Strictly speaking, AR is a broad concept including all associated technologies, devices (i.e. head mounted display, wireless wristband, digital camera, or wireless sensor, etc.), interfaces (i.e. tangible, collaborative or hybrid interfaces), and systems (i.e. indoor, outdoor or mobile systems), which are used to display, input, track, and output information [1].

QR code (Quick Response Code) is one of the AR techniques and was initially invented for the automotive industry in the early 1990s[3]. Similar to bar codes, QR codes technically are machine-readable optical labels using matrix barcode or two-dimensional barcode to store information of the item to which it is attached. The data in a QR code is stored in the form of four standard encoding modes such as numeric, alphanumeric, byte/binary, and kanji [2]. Graphically, a QR code consists of black modules arranged in a square grid on a white background, including five areas: finder pattern, alignment pattern, timing pattern, quiet zone, and data area [2]. Each area has its unique functionality. For instance, Finder pattern are the squares in the outermost corners and used to help the image device (such as camera) to determine the position, angel, and size of a QR code. Alignment pattern are the squares in the middle and used to detect the distortions of a QR code. Timing pattern are the dotting lines to connect finder pattern squares and used to determine the coordinates of a QR code and ensure that it has not been

[1] http://www.internetlivestats.com/internet-users/

[2] http://www.searchenginejournal.com/2014-mobile-landscape-25-statistics-will-drive-future-mobile-marketing-infographic/89507/

[3] http://en.wikipedia.org/wiki/QR_code#cite_note-QRCodefeatures-1

distorted. Quiet zone is the blank area around a QR code to isolate the QR codes from its background. Data area is the light grey area and used to encode data in the binary numbers of 0s and 1s based on Reed-Solomon codes.

The goal of this study is to explore one of the functions of QR codes—information protection, especially usernames and passwords. It is a trend to introduce QR codes into online account protection. A report in 20124 shows that nearly 58% of adults have 5 or more unique online passwords among which 30% have 10 or more and 8% have a whopping 21 or individual passwords. It is broadly admitted that having different passwords for each individual web account is an effective way to protect our information as well as accounts. However, this password strategy is challenged by daily increased online activities. For example, if a user has 10 accounts online, a regular updates of his/her passwords would become a heavy burden. In addition, some users would think if it is unsafe to use a public computer to login into their accounts. Some web-service providers such as Gmail propose to use QR function in smartphones as a peripheral approach to verify their users' identity, considering the popularity of smartphones and similar electronic devices.

The use of QR codes in information protection relies on the collaboration of computers and mobile devices. Any electronic devices with cameras and QR apps would a good tool to use. Technically, the users of QR codes need to open up the webpage that they intend to login on computers and, in the meanwhile, turn on QR reader in their mobile devices. The web on the computer would provide a QR code, and the QR reader on the mobile device scans the code and sends a feedback to the webpage. Once the webpage receives the feedback from the QR reader, the whole login process is completed. Regarding the usernames, there is no need to type them at all. Regarding the passwords, there are in general two approaches to handle it. One type of webportals such as Gmail still requires their end users to type in their password on their mobile devices. Contrarily, the webportals such as Weixin (or WeChat) completely do not require passwords when using QR codes to login.

Using QR codes to login is still a new technique to use for many end users as well as webportals. Our study contributes to the extant literature for two reasons. First of all, we measure the functions of QR codes in information protection from a theoretical lens. Although some companies have already put QR codes into practice on their login webpages, it is still obscure that how these QR codes would help their users to increase their perception of being secured. We integrate two theories—protection motivation theory (PMT) and theory of planned behavior (TPB)—to study this effect. We think these two theories would be effective tools to gauge the effect of QR code on information protection, since both of the theories are commonly adopted to study the phenomena of information security and privacy. The integration of these two theories would perfectly measure the cognitive processes pertaining to the use of QR codes. Secondly, the studies help the practitioners understand how QR codes mitigate end users' fear. It is assumed that QR codes could reduce end users' fear of losing their private information. But how does this work? How much would this effect be? This study will provide a picture of the mechanism generated by QR codes.

Hence, the rest of paper is organized as follows. We first discuss the theoretical background regarding the two aforementioned underlying theories. Second, we propose the hypotheses to be measured in the study and related research model.

THEORETICAL BACKGROUND

[4] http://janrain.com/about/newsroom/press-releases/online-americans-fatigued-by-password-overload-janrain-study-finds/

- **Protection Motivation Theory (PMT)**

PMT was developed to explain the fear-related cognitive process [3] and has been broadly adopted by IS researcher to explain end-users' intention to adopt information-security-related measures, such as anti-malware software, anti-plagiarism software, and information security polices and son on [4]. PMT was rooted in expectancy-value theories and proposed to study on people's psychological reactions to potential threats [3]. It theorizes that, in a noxious situation, a fear appeal will initiate a cognitive meditational process and ultimately cause a change in attitude. A fear appeal consists of three components: magnitude of noxiousness, probability of occurrence, and efficacy of recommended response [3]. It also theorizes that an individual's intention to protect from potential threats is affected by two appraisal processes: threat appraisal and coping appraisal. Specifically, the threat appraisal examines the maladaptive behavior (such as fear, perceived severity, and perceived vulnerability), and the coping-appraisal process examines the efficacy of the preventive behavior that an individual may carry out and the individual's perceived ability (such as self-efficacy, response efficacy, perceived ability to control, and personality traits) [5].

- **Theory of Planned Behavior (TPB)**

In addition to fear appeals, we are also interested in examining the intermediate cognitive process leading to end-users' intention to adopt. Consequently, the second theory to use is the theory of planned behavior (TPB). TPB is a broadly accepted theory to study people's intention to adopt certain behaviors/counter-measures. Theoretically, it believes that a person's volitional behavior is affected by his/her motivation (e.g. behavioral intention), ability, and joint effects of attitude, subjective norm and perceived behavioral control (PBC) on his/her motivation [5]. For instance, it finds that the attitude, subjective norm and PBC toward either getting information or purchasing itself impact an online shopper's final decision on purchase[6]. Regarding the adoption of QR codes, we believe it has some commonality with the adoption of other new technologies. End-users' belief on controlling the new technologies, the influence from close friends, and their attitude toward the new technologies will definitely impact their final decision on adoption. Therefore, we apply TPB to examine the related decision making procedure.

HYPOTHESES AND RESEARCH MODELS

In line with the integration of two theories, the study examines the functions of QR codes in two stages. We first measure the cognitive mediating process related to fear appeals. According to PMT, this cognitive process consists of two sub-processes ─ threat appraisal process and coping appraisal process. In particular, the threat appraisal process is constituted by two factors ─ perceived threat severity and perceived threat susceptibility and the coping appraisal process have three factors ─ self-efficacy, response efficacy, and response cost. We second measure how this attitude influence the final intention to adopt QR codes as well as peripheral perceptions as indicated by TPB. Therefore, in this study we propose the following hypotheses.

- **Perceived Threat Severity**

One of the factors in threat appraisal process is the perceived threat severity, which measures the degree to which a person believes a threat will be severe to his or her life [5]. Rationally, the more severe the negative consequence of a certain behavior is perceived to be, the more likely that person will adopt recommended behaviors or measures. That is, if end users feel that the security of their private information such as username and password is threaten, they would like to adopt the recommended

measures to protect their information. Oppositely, no protection would be aroused if there is no threat being sensed.

In our context, logon onto an account in an unknown environment involves a potential threat to lose end-users private information. Many accounts are linked with bank account and credit card information. We believe that the exposure of those information would cause a sever outcome, and the adoption of QR codes could reduce such an opportunity. Therefore, we hypothesize that, in regard to account protection, perceive severity of potential threat would have a positive effect on end-users' attitude toward the adoption of QR codes.

H1: Perceived threat severity has a positive effect on end-users' attitude toward QR codes adoption.

- **Perceived Threat Susceptibility**

The second factor in threat appraisal process is perceived threat susceptibility, which measures an individual's estimation on potential likelihood of a threat would affect his or her [4]. For example, if an end-user suspects that the installation of a given App on his/her smartphone would cause the exposure of his/her private information, it is very likely for him or her not to install that app in the very beginning. Following the logic, we hypothesize that

H2: Perceived threat susceptibility has a positive effect on end-users' attitude toward QR codes adoption.

- **Self Efficacy**

Self efficacy measures an individual's belief that he or she has the ability to cope with or perform a given behavior. Past studies indicate that when a user feels capable to manipulate a new technology, it is more likely for him or her to adopt this technology. In the context of this research, QR codes in the information security realm are still a new concept. Not many end-users are familiar with this technique, especially those non-smartphone users. This belief of being capable to control QR codes rationally has an impact on end-users attitude. Following the prior study, we hypothesize that

H3: Self efficacy has a positive effect on end-users' attitude toward QR codes adoption.

- **Response Efficacy**

Response efficacy measures an individual's belief of the effectiveness of a given behavior on alleviating a threat [4]. For example, if a end-user believes that a certain anti-malware software is effective on securing his/her computer, the intention for him/her to install this software would be consequently high [7]. In our context, the response efficacy refers to end-users' belief that QR codes can effectively help them protect their account information. As such, we hypothesize that

H4: Response efficacy has a positive effect on end-users' attitude toward QR codes adoption.

- **Response Cost**

Response cost measures any associated cost for taking adaptive coping response [4]. Such cost may include any monetary expense, time costs, and other inconvenience pertaining to the adoption of a behavior. For example, in many cases, to adopt a new technology, the end-user may need to receive training, purchase new devices, and install new software and so on. Any efforts related to the adoption of this technology are regarded as response cost. Rationally, an end-user may be reluctant to change his/her current technology in use, if the response cost is high for adopting a new one [7]. Therefore, we hypothesize that

H5: Response Cost has a negative effect on end-users' attitude toward QR codes adoption.

- **Attitude**

The attitude in TPB measures an individual feeling (either positive or negative) towards engaging a given behavior [8]. It reflects an overall assessment of a given object or behavior. In traditional IS researches, it shows that the attitude toward the adoption of a IS technique has a positive effect on its final adoption [7]. QR codes are regarded as a technique to protect account information. Therefore, we hypothesize that

H6: Attitude toward QR codes has a positive effect on end-users' intention to adopt.

- **Subjective Norm**

Subjective norm measures an individual's perception of social normative pressures that he or she should or should not perform an action to follow the opinions from influential peers such as friends, colleagues and relatives[5]. TPB suggests that people who are close to an individual (such as bosses, colleagues and parents) has a certain power to impact his/her behaviors. For example, in a company, the opinions from boss, colleagues, subordinates and even IT department can influence an individual's compliance to a new security policy[8]. Subject Norm is an important factor to consider in technology adoption. Therefore, we hypothesize that

H7: Subjective Norm has a positive effect on end-users' intention to adopt.

- **Perceived Behavioral Control**

PBC measures an individual's perceived controllability of behavior based on experience and abilities to carry out the behavior [5]. TPB suggests that when an individual feels that he has sufficient capability to carry out a given behavior, it is very likely for this person to eventually perform this behavior. Many IS studies have confirmed this belief [8]. Therefore, in our context, we hypothesize that

H8: Perceived behavioral control has a positive effect on end-users' intention to adopt QR codes.

Overall, integrating all the aforementioned hypotheses, we propose a theoretical model as shown in Figure 1.

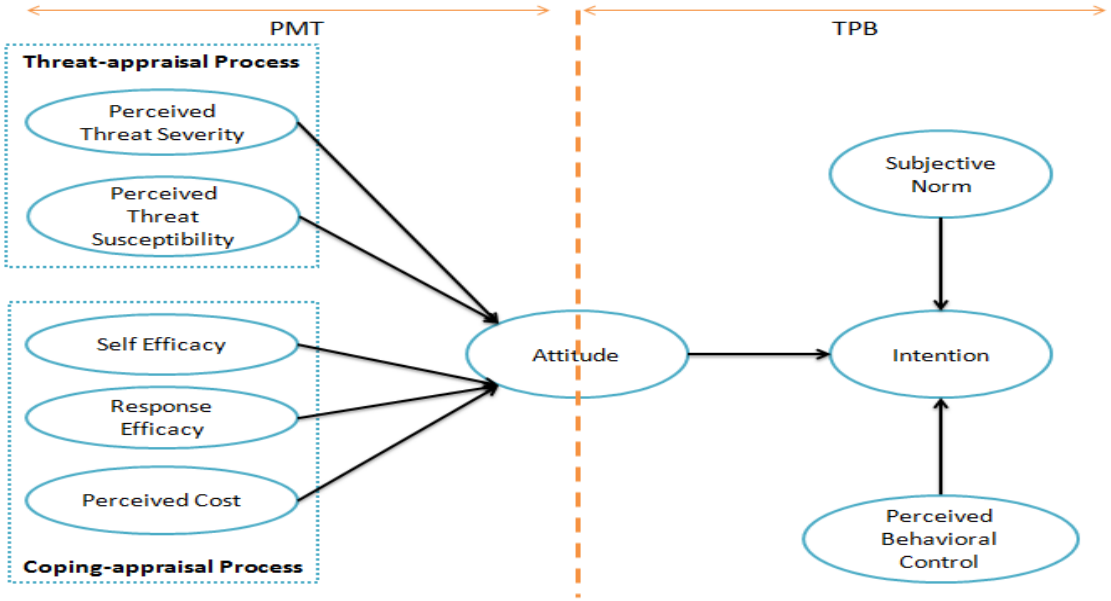

Figure 1. Research Model

REFERENCES

[1] Carmigniani, J. and B. Furht, *Augmented Reality: An Overview*, in *Handbook of Augmented Reality*, B. Furht, Editor. 2011, Springer: New York. p. 3-46.

[2] Kan, T.-W., C.-H. Teng, and M.Y. Chen, *QR Code Based Augmented Reality Applications*, in *Handbook of Augmented Reality*, B. Furht, Editor. 2011, Springer: New York. p. 339-354.

[3] Rogers, R.W., *A Protection Motivation Theory Of Fear Appeals And Attitude Change.* Journal of Psychology, 1975. **91**(1): p. 93.

[4] Crossler, R.E., et al., *Understanding Compliance with Bring Your Own Device Policies Utilizing Protection Motivation Theory: Bridging the Intention-Behavior Gap*, in *Journal of Information Systems*. 2014, American Accounting Association. p. 209-226.

[5] Lixuan, Z. and W.C. McDowell, *Am I Really at Risk? Determinants of Online Users' Intentions to Use Strong Passwords.* Journal of Internet Commerce, 2009. **8**(3/4): p. 180-197.

[6] Pavlou, P.A. and M. Fygenson, *Understanding and Predicting Electronic Commerce Adoption: An Extension Of the Theory Of Planned Behavior.* MIS Quarterly, 2006. **30**(1): p. 115-143.

[7] Meso, P., Y. Ding, and S. Xu, *Applying Protection Motivation Theory to Information Security Training for College Students.* Journal of Information Privacy & Security, 2013. **9**(1): p. 47-67.

[8] Ifinedo, P., *Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory.* Computers & Security, 2012. **31**(1): p. 83-95.