The Effectiveness of Fear Appeals in Increasing Smartphone Locking Behavior among Saudi Arabians

Elham Al Qahtani and Mohamed Shehab, ***University of North Carolina Charlotte;***
Abrar Aljohani

https://www.usenix.org/conference/soups2018/presentation/qahtani

This paper is included in the Proceedings of the Fourteenth Symposium on Usable Privacy and Security.

August 12–14, 2018 • Baltimore, MD, USA

ISBN 978-1-939133-10-6

Open access to the Proceedings of the Fourteenth Symposium on Usable Privacy and Security is sponsored by USENIX.

The Effectiveness of Fear Appeals in Increasing Smartphone Locking Behavior among Saudi Arabians

Elham Al Qahtani
College of Computing and Informatics
UNC Charlotte
ealqahta@uncc.edu

Mohamed Shehab
College of Computing and Informatics
UNC Charlotte
mshehab@uncc.edu

Abrar Aljohani
johani.abrar@outlook.com

ABSTRACT

Saudi Arabia has witnessed an exponential growth in smartphone adoption and penetration. This increase has been accompanied with an upward trend in cyber and mobile crimes. This calls to efforts that focus on enhancing the awareness of the public to security-related risks. In this study, we replicated the study performed by Albayram et al. [14] published in SOUPS 2017; however, our study targetted participants in Saudi Arabia. We also investigated different fear appeal video designs that were more suited for this population (customized video, Arabic dubbed, and captions for the original video). The results from the original study, conducted in the United States, showed that 50% of participants in the treatment group and 21% in the control group enabled screen lock. The reason for replicating the original paper was to increase Saudis' awareness regarding the importance of sensitive data, especially with the increasing level of cybercrime. Our results showed that the Saudi-customized video was extremely effective in changing our participants' locking behavior (72.5% of participants enabled the screen lock), based on customized applications and Saudi culture. The dubbed video was the second-most effective (62.5%) locking behavior. Finally, we have illustrated our data comparison analysis in detail.

1. INTRODUCTION

In Saudi Arabia, there has been an exponential grown in the use of smartphone technologies. According to a report by the Saudi Ministry of Communication & Information Technology [5], in 2001 the number of mobile subscriptions in Saudi Arabia was around 2.5 million (12% mobile penetration). By 2017, the number had risen to 43.63 million with a population penetration rate of 137%, which is the highest mobile penetration rate in the region [26]. In Saudi Arabia, the mobile banking penetration is 81%, which is considerably higher than other developed and emerging Asian nations [6]. In addition, Saudis are increasingly using smartphone applications to conduct business and communication.

With this increase, cyber threats are becoming more common as 58% of the Saudi population have experienced some form of online cyber crime in the past year, and one in four users have had their mobile device stolen, potentially exposing sensitive information in their e-mail, social media and banking apps to cyber thieves [3]. Kaspersky Security statistics showed that 53.1% of Saudi users were affected by local threats (malware spread in local networks, by USBs, CDs, DVDs) [7]. In 2018, the Saudi government statistics showed an increase in online blackmail, where extortionists demanded money, sex and many other demands from their victims [4].

In response to these cybersecurity challenges, there have been several efforts lead by both the public and private sectors to provide security tools, education, and awareness to the Saudi population. For example, the organization responsible for awareness of Saudi companies, government organizations, and society in Saudi Arabia is the National Center for Cybersecurity [9]. It aims to educate Saudis about the dangers of using the Internet, the social communication and the loss of personal information through awareness lectures, workshops, and social media. We believe that the security and privacy problems in Saudi Arabia are further exacerbated by the lack of security awareness of the population. Alzahrani et al. [16] stated that 92% of Saudis had never attended security training. Recently [10, 11], the Saudi Federation for Cyber Security has provided educational and awareness programs in Saudi Arabia.

As there are several types of proprietary data storage in mobile phones, screen lock techniques are effective in protecting mobile content and preventing strangers from gaining unauthorized access, which could lead to extortion via the threat of destroying the victim's reputation. Several researchers [37, 29, 36, 23, 45] have noted the important relationship between applying a screen lock mechanism and users' motivation and risk perception. A study of smartwatches by Nguyen et al. [38] used similar concepts to evaluate different locking mechanisms. For effective security and improved user experience, Ohana et al. [40] found that combining biometric identification (e.g., fingerprint, face, or voice recognition) with other security lock mechanisms improved security.

Our paper replicates the study performed by Albayram et al. [14] for two main reasons: the lack of security training leads to 92% of Saudi society to be not aware of the importance of security and its potential consequences [16], and cybercrime (e.g., blackmail) is increasing in Saudi Arabia [4]. For this reason, we decided to investigate if we could improve the efficiency of communicating risk to the Saudi population.

USENIX Symposium on Usable Privacy and Security (SOUPS) 2018.
August 12–14, 2018, Baltimore, MD, USA.

The original study compared the smartphone locking behavior of a treatment group that watched a fear appeal video to that of a control group. That online study found that 50% of the treatment group enabled the screen lock compared to 21% of the control group. In this paper, we replicated the original study and did so with a Saudi population of mobile users through an in-person study with 200 Saudi participants. We also investigated various video designs that were more suited to the Saudi population (customized video, Arabic-dubbed video, and Arabic-captioned video) in the context of smartphone locking behavior. We found that 72.5% of participants who watched the customized video enabled the screen lock, as compared to 62.5% of those who watched the dubbed video, 42.5% of those who watched the subtitled video, and 20% of those who watched the original video. In contrast, among the control group that was not shown any video, 17.5% enabled the screen lock.

This paper is organized as follows. Section 2 discusses the original study. Section 3 discusses related work. Section 4 describes the methodology. The study results are presented in Section 5. Section 6 presents the study discussion. Section 7 discusses limitations and suggestions for future work. Section 8 concludes our paper.

2. THE ORIGINAL STUDY

In the original study, Albayram et al. [14] discussed how effective risk communication leads to a change in users' risky behavior, rather than simply annoyance among users. The authors designed a video that targeted people who did not use a screen lock on their smartphone. They sought to determine whether this video would affect users' locking behavior and change their attitude about enabling a screen lock. The video explained the risks of having their data stolen if users did not activate a screen lock mechanism on their smartphone. The video was based on guidelines for four appeals to fear from the protection motivation theory [42, 47], as follows: (1) perceived severity (perception of the seriousness of threat), (2) perceived vulnerability (possibility incidence of threat), (3) self-efficacy (confidence about taking the recommended action), and (4) response efficacy (perception of the efficacy of the recommended action).

In that study, the participants were divided into a treatment group that watched the video and a control group that did not watch the video. The study was conducted through Amazon's Mechanical Turk and was divided into two phases, as follows:

1. The main study included three parts with several kinds of questions: both groups were asked questions about demographics, smartphone usage behavior, online security behavior, and reasons for not using a screen lock on their smartphone. Questions about the video evaluation were only asked to the treatment group. The two groups were also asked questions about security and privacy concerns, the perceived value of their data, risk perception, response cost, and response efficacy.
2. The follow-up study included questions for both the control and the treatment group about whether they had enabled a screen lock and what their reasons were for doing so or not doing so.

Albayram et al. [14] found that the informative fear appeal video specified for the treatment group was effective at changing users' locking behavior and risk perception based on fear appeals elements. After conducting the follow-up study, they found that 50% of participants in the treatment group and 21% in the control group had enabled a secure screen lock on their smartphone.

3. RELATED WORK

Two kinds of research are relevant to our study: that dealing with cultural context and that dealing with risk communication techniques.

3.1 Cultural Context

In this section, we clarify how cultural differences play an important role in changing society's behavior, such as national culture, cognitive differences, and laws. The two following studies illustrate significant differences in different populations. A replicated study performed by Mayer et al. [35], conducted a comparison of password composition policy (PCP) samples from U.S. and from German websites. One of their findings was that German websites had lower PCP strengths than did the U.S. samples. Another study performed by Nishi et al. [39] conducted an online experiment using economic games among 337 Indian users, 1,059 American users, and 66 users from other countries. They found that American culture played an important role in users' lives. Based on this, users quickly made decisions involving highly mutual assistance compared to others in online social environments. Regarding national culture, Salter et al. [43] found that the simple national culture effect was important even between societies with similar cultures (e.g., the U.S. and Canada). Using the agency theory of human behavior patterns, for example, American managers had a higher rate of adverse decisions than Canadians. A study performed by Kitayama et al. [33] examined decision making and cultural differences in cognition using a framed-line test that compared Japanese (an East Asian culture) and Americans (a North American culture). They found that Japanese made more accurate decisions than Americans. In addition, laws have a significant influence on a person's behavior; for example, the Kingdom of Saudi Arabia is a conservative society and applies gender segregation [34] in higher education, banks, mosques, and restaurants.

3.2 Risk Communication Techniques

It is important to understand smartphone users' perspective on security and their perception of the seriousness of risk. Egelman et al. [22] examined the security behavior intentions scale (SeBIS), which measures users' behavior in regard to computer security. The SeBIS was used to rate user awareness, password strength, updates on security, and securement mechanisms. Several studies have investigated risk communication methods using videos, graphics, text, symbols, and messages to measure the effects on users' risk perception and behavior [13, 14, 19, 28, 32, 41]. For example, Pattinson and Anderson [41] examined risk communication methods and symbols and graphics included in information security messages. They found no significant improvement in risk communication using this method. Bravo-Lillo et al. [19] performed three experiments using a computer security dialogue with five attractors to attract user attention focusing on the perception of cost. However, they found that interacting with only two inhibitive attractors by swiping over the text and typing in the text box was effective

in reducing the incidence of users' ignoring the appropriate action for granting permission, based on habituation that taught users how to achieve the task and speeded up their responses to a dialogue.

A study performed by Yousra et al. [32] investigated the use of an animated dialogue to attract users' attention toward granting permissions through a non-inhibitive attractor which highlighted personal information in the color red. They found that, compared to the control and to checkbox dialogues, the proposed animated dialogue had a significant impact on the duration of users' looking at the personal information, users' concern about their data, and users' understanding of the purpose for each permission. A study by Harbach et al. [28] investigated risk communication using personalized examples of permissions for Android applications and found that such communication affected users' decisions by making them aware of potential risks. In 2017, two studies conducted by Albayram et al. [13, 14] used effective risk communication by a video to raise user awareness of security and privacy and to motivate users to follow recommended security procedures. Albayram et al. [14] evaluated the effect of a fear appeal video on users' perceptions and behavior in terms of enabling a secure screen lock mechanism. In addition, Albayram et al. [13] investigated the effect of leverage videos about enabling two-step verification (2FA) on users perceptions and attitudes, seeking to motivate them to be familiar with security tools and updated new security advice.

4. METHODOLOGY

The purpose of the present study is to examine the effectiveness of fear appeal videos in changing Saudi Arabians' risk perceptions and raising their awareness. In addition, based on the videos' effectiveness, we want to investigate if there are changes between the users' initial reasons for not using a screen lock and their reasons in the second round follow-up study. The following sections describe the video design for the present study, the hypotheses, and the study design.

Figure 1: A frame from the customized video content

4.1 Video Design

Researchers in the education field have shown that videos are highly effective in attracting users' attention and in making salient features clear [20, 30, 46], and studies have measured the changes videos make in users' perceptions [13, 14, 18, 25]. In order to study the effectiveness of video media on communicating fear appeal to the Saudi population, we designed a customized video targeting the Saudi audience that gave participants an explanation of the expected risks of not using locking mechanisms [31] and a short demonstration of how to add a lock to their phone, based on security advice from Android [12, 17, 44] and iOS [1]. The duration and topic of the customized video were similar to that of the video in the original study (the original video was 3 minutes long). The videos were customized with scenarios and content to ensure relevance to the Saudi audience. The scenarios were applied to the perception of the data value, the perceived vulnerability about Saudis smartphones' security and privacy, the perceived cost that connected to Saudis' decisions of following the recommended tips and self-efficacy that was based on their belief of the suggested tips [42]. The customization focused on the following aspects:

- **Relevant Risks and Fears:** This aspect focuses on ensuring the video targets risks and fears that are related to the target audience and that would clearly communicate threats. For example, the video was customized to present a scenario in Arabic in which a victim is being deceived and blackmailed via stored personal media in WhatsApp messages, which is aligned with the popularity of online blackmail and extortion crimes in Saudi Arabia. In addition, the video demonstrated the risks of exposing media stored in smartphone photo albums and discussed the risk of reputation damage specially in a conservative society. Regarding self-efficacy, the customized video illustrated the steps of enabling a secure lock screen on iPhone and Android phones with Arabic settings on the smartphone. All these scenarios would be familiar to the Saudi population.

- **Relevant applications and attributes:** The video was updated to include smartphone applications and attributes that are common in Saudi Arabia. The video was customized to include information related to the top-ranking applications among Saudis [8] (e.g., WhatsApp, Snapchat, Instagram, and ALRajhiBank (a popular Islamic bank [2])), rather than those used in the original video (Paypal, Netflix, Bank of America app, and Amazon). We presented an ALRajhiBank scenario in which the victim's bank information was stolen by sending a 2FA code to the victim's stolen device and accessing the bank password and username stored on the victim's smartphone. We also included a scenario using Whatsapp. Attributes focus on data attributes that are relevant to the target population, for example the national identity number was used instead of social security number which was used in the original video. The customized video also demonstrated the steps to enable a secure screen locking method using device settings in Arabic, both for Android and for iOS, whereas the original video only included Android's screen lock set up.

- **Cultural:** The video should also be culturally relevant, which was ensured by customizing the video dialog to use culturally relevant vocabulary delivered in Arabic. In addition, the video used photos of men and women in the Saudi dress taking into consideration the ideology of the conservative society.

The main goal was, to customized the video content, to ensure the participants felt that it is relevant their mobile

experience and their security. The narrator of the Saudi-customized video was one of the authors of this paper, and the transcript of the customized video is in the Appendix. Figure 1 shows a frame from the customized video content that is related to Saudi culture.

The study examined five groups–four treatment groups and a control group, as described below:

- Original group (Treatment Group 1): watched the video in English used in the original U.S. study.
- Dubbed group (Treatment Group 2): watched the original video but with Arabic dubbed. Figure 2 (a) shows a frame from the Arabic-dubbed video. [1]
- Subtitled group (Treatment Group 3): watched the original video but with Arabic captions. Figure 2 (b) shows a frame from the Arabic-captioned video. [2]
- Customized group (Treatment Group 4): watched a Saudi-specific video in Arabic. Figure 2 (c) shows a frame from the customized video. [3]
- Control group: did not watch any video.

We assigned the original video to one group to test whether it changed Saudi locking behavior or perceptions based on its visual content, ignoring the English dialogue; our measurements depended on the effectiveness of the video's content (the applications used in the video, the dialogue in the video). As Saudi participants might not understand the original video due to the unfamiliar smartphone applications and the English dialogue, we added Arabic captions and dubbed the original video, assigning these to the subtitled group and the dubbed group, respectively, to test whether these changes would affect Saudis' perceptions.

The customized and dubbed videos significantly affected Saudis' locking behavior on perceived severity, vulnerability, and response efficacy. The rating for the perceived inconvenience of using the secure screen lock was also considerably lower for both groups compared to the original, the subtitled and the control groups.

4.2 Hypotheses

In the present study, we propose the following hypotheses:

Hypothesis 1 (H1): There will be significant differences among groups in their ratings of perceived sensitive data (H1a). The group that watched the Saudi-customized video will have higher ratings on perceived sensitive data than will the other treatment groups, and all the treatment groups will be higher than the control group (H1b).

Hypothesis 2 (H2): There will be significant differences among groups regarding concerns about their smartphones' security and privacy and about their data being used by other people (H2a). The customized group will have a higher level of concerns about their smartphones' security and privacy and their data being used by other people than will the other treatment groups, and all the treatment groups will be higher than the control group (H2b).

[1] https://youtu.be/5OpZ2jVGxRY
[2] https://youtu.be/4P91WgGH-r4
[3] https://youtu.be/g-IlWrvmRF4

Hypothesis 3 (H3): There will be significant differences among groups in their ratings of perceived severity and risk awareness (H3a). The customized group will have higher ratings of perceived severity and risk awareness than will the other treatment groups, and all the treatment groups will be higher than the control group (H3b).

Hypothesis 4 (H4): There will be significant differences among groups in their ratings of the perceived response cost (H4a). The customized group will have lower ratings of perceived response cost than will the other treatment groups, and all the treatment groups will have lower ratings of the control group (H4b).

Hypothesis 5 (H5): There will be significant differences among groups in their ratings of response efficacy (H5a). The customized group will have higher ratings of response efficacy than will the other treatment groups, and all the treatment groups will be higher than the control group (H5b).

Hypothesis 6 (H6): There will be significant differences among groups regarding the number of participants who enabled a screen lock (H6a). The customized group will have a higher number of participants who enabled a screen lock than other treatment groups, compared to the control group (H6b).

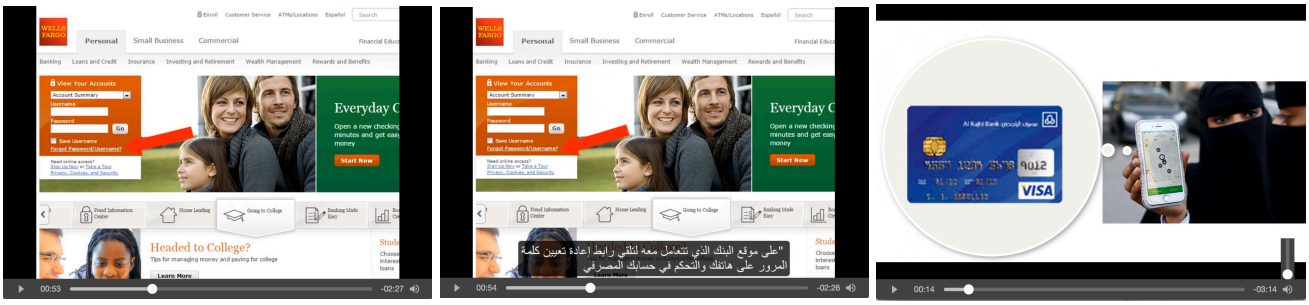
4.3 Study Design

The present study was conducted in person, whereas the original study was an online study. For the present study, we recruited Saudi participants who were at least 18 years old, owned a smartphone that provided a secure screen locking mechanism, and did not activate the screen locking mechanism on their phone. For example, we excluded Saudis who had old cell phones that did not support screen-locking mechanisms. We collected participants' cell phone numbers and used those numbers to call the participants in order to follow up after the study and investigate whether they had enabled screen locking; we then deleted participants' phone numbers after the follow up call was made. The participants were recruited through flyers and through face-to-face recruitment. When administering the study, we did not provide any explanatory information to the participants but instead asked them to watch a video and answer survey questions afterward.

The present study applied the same questions as did the original study, but they were translated into Arabic to fit the Saudi population; the administered translated survey can be seen in the Appendix. The process of the study design, which included a first round of a main study and then a second round with a follow-up study, was as follows.

4.3.1 First Round: The Main Study

We interviewed 200 Saudi participants individually (an in-person study) who met our inclusion criteria; the participants were assigned randomly to one of the five groups to prevent self-selection bias. After obtaining user consent, we explained the purpose of our study and collected participants' phone numbers to use for the second round of the study. Each group included 40 Saudi participants. We met them in public places (e.g., outside prayer areas, shopping malls, schools, and hospital waiting areas). Our study was conducted in different cities in Saudi Arabia. Responses to the questions were recorded in the questionnaire to ensure



(a) Arabic dubbed (b) Arabic captions (c) Customized video

Figure 2: Screen shots of the different videos

that we received accurate responses. We let participants watch a complete video based on their random assignment to groups. All Arabic responses were translated into English.

During the first round of the main study, we asked participants three sections of questions. The first section was background questions, smartphone usage behavior questions, online security behavior questions, reasons for not using a screen lock, and their opinions about people who use a lock screen on their smartphone. The second section was only for those in the treatment groups, who watched a video; we asked them about the video's effects and their evaluation of the video. The control group were not shown a video, and hence they were not asked the questions in the second section. All five groups were asked the third section, which included questions about data value, security and privacy concerns, risk awareness, response cost, and response efficacy. The average total time of our interviews with members of the groups who had watched the video was approximately 20 minutes, including 3 minutes during which participants watched the video, whereas the duration of the interviews with members of the control group was around 15 minutes.

4.3.2 Second Round: The Follow-Up Study

We followed up with the participants a week after their initial interview to evaluate whether they had enabled a screen locking mechanism on their phones and to learn the reason behind their choice. This second interview was performed using a follow-up the questionnaire and was conducted by phone or in a location agreed upon with the participant.

Our study was approved by UNC Charlotte's Institutional Review Board [1] and the Saudi Arabia regulatory committee.

5. EVALUATION

Since our data was ordinal, we used non-parametric tests for the analysis. In comparing all the groups independently, we used the Kruskal-Wallis test (H) in an equal sample size [24]. We also used post hoc multiple comparison to compare groups for each research question. To avoid Type I error (alpha) in testing our significance, we used the adjusted significance for Bonferroni at (0.05) [21]. All analysis was done using the Statistical Package for the Social Sciences (SPSS).

5.1 Sample Statistics

Based on our data analysis of the Saudi population, we assigned an equal number of people of each gender to each group (20 male and 20 female), so that there was no significant difference among five groups in terms of gender. We performed the Kruskal-Wallis test and found no significant differences among all groups regarding the following demographic characteristics: age ($H(4) = 3.881$, $p = .422$), education level ($H(4) = 4.512$, $p = .341$), level of computer knowledge ($H(4) = 4.35$, $p = .365$), and participants' language ($H(4) = 5.191$, $p = .268$).

In terms of smartphone usage behavior, there were no significant differences among the five groups when we asked them five questions about their smartphones' operating system type ($H(4) = 2.576$, $p = .631$), number of times using their smartphones during the day ($H(4) = 4.654$, p = .325), number of applications on their smartphones ($H(4) = 8.921$, $p = .063$), number of times they used these applications ($H(4)= 6.078$, $p = .193$), and the applications they used daily ($H(4) = 2.774$, $p = .596$).

In comparing online security behavior among all five groups, we found no significant differences in concerns about their online accounts being hacked ($H(4) = 5.837$, $p = .212$). All groups had no concerns about online security ($H(4) = 4.019$, $p = .403$) and whether they used antivirus software security ($H(4) = 7.040$, $p = .134$).

5.2 Reasons for Not Employing a Screen Lock

In the questionnaires first section, we asked participants their initial reasons for not employing a lock screen on their smartphones and their opinions about why people use screen locks on their smartphones. For the question related to the initial reasons for not employing lock screen we updated it to a multiple choice question using the coding results that were concluded by the original study as choices, we also added a "other" option for participants that have a reason not included in the listed choices.

In comparing the responses of all five groups, we found no significant differences in the reasons for not employing a screen lock among the treatment groups and the control group ($H(4) = 2.707$, $p = .608$), as 30% of participants in all groups agreed on the top reason, "Annoying to use" [14, 23, 27, 29], 22% chose "Nothing to hide" as their reason, 21.5% chose "No risk", and 17% chose "Forgettable/mental burden." The least common answer was "Don't know how to set up", chosen by 5% of participants in all groups. The ranking of reasons was similar to that found in the original study.

[1] IRB Protocol #17-0426

For instance, a comment from the customized group said, "I share my phone with my mother and sister, especially when using Internet data by connecting through a personal hotspot." A participant from the original group reported not locking the phone "because my children continue to press the secret code by mistake and that hangs up the mobile for a long time when I might need to use my mobile immediately. In other words, I do not use it to avoid suspending the screen." The control group comments included, "Annoying, and there are tools that unlock passwords easily."

We noticed in the interviews when we asked participants why they thought people used a secure lock, participants' reasons were related to their misconceptions about using a screen lock and a failure to recognize the importance of their sensitive data. For example, a Saudi participant over 60 years old from the original group mentioned that lock users "hide inappropriate information, such as forbidden photos inside their phone, and if you are confident you will not hide anything from your family." A participant from the dubbed group said those who locked their phones wanted to "protect their calling balance from anyone using it." One from the customized group commented, "Maybe they have bad photos on their phones and misfortunes to hide from others." In a different vein, someone from the control group replied, "They know how to use this technology."

5.3 Impact of Fear Appeals on Fear of Losing Sensitive Data

We assumed that there were significant differences among the groups in their ratings of perceived sensitive data (H1a), and that the group that watched the Saudi-customized video would have higher ratings on perceived sensitive data than the other treatment groups, which would be higher than the control group (H1b).

To test the first hypothesis (H1), which included (H1a) and (H1b), we asked participants in all the five groups two questions related to their perceived sensitive data. The first question was, "Do you think that data stored in your smartphone is valuable enough to protect?" The second question was, "How much privacy-sensitive data do you think your smartphone stores?" The answers were measured on a scale ranging from (0) "None at all" to (3) "A great deal of privacy-sensitive data."

Performing the Kruskal-Wallis test among all five groups, we found significant differences for both questions at $p \leq .001$ for the first question ($H(4) = 22.58$ with a medium effect size, $\eta^2 = 0.11$), for the second question ($H(4) = 24.88$ with a medium effect size, $\eta^2 = 0.12$).

For the first question, differences were found at an adjusted significant level $p \leq .001$ by performing the Bonferroni multiple comparisons tests between the original and the customized group and between the control and the customized group. We found that 95% of participants from the customized group, 80% from the dubbed group, 67.5% from the subtitled group, and 55% from both the original and the control groups chose "Yes," depending on the priority.

For the second question, we found significant differences when performing the Bonferroni multiple comparisons test with adjusted significance and mean rank, which used to compare the effect of the different of each group, as shown in Table 1. Among participants in the dubbed group (median = 2), 37.5% believed their smartphones had a moderate deal of privacy-sensitive information, whereas 42.5% of those in the customized group (median = 2) thought their smartphones had a great deal of privacy-sensitive information. Among those in the subtitled (median = 1), original (median = 1), and control groups (median = 1), 32.5%, 45%, and 42.5%, respectively, rated the amount of sensitive data they had as "None at all."

"How much privacy-sensitive data do you think your smartphone stores?"	
Comparison of Groups (Mean Rank)	**Adj. Sig.**
Control (81.6) vs. Customized (131.6)	$\leq$.001
Original (82.1) vs. Customized (131.6)	$\leq$.001
Subtitled (92.2) vs. Customized (131.6)	.016

Table 1: Post hoc test of the second question on sensitive data

Participants' varying ratings of the importance of the data stored on their smartphones, especially for the treatment groups, demonstrated the impact level of the fear appeal of the videos, and these changes reflected participants' perceptions about the importance of the personal data they had on their smartphones. The results of the customized and dubbed groups demonstrated a significant change in behavior compared to the other groups' ratings of their phones as having either "A moderate amount" or "A great amount" of sensitive data. Thus, both H1a and H1b were supported.

5.4 Impact of Fear Appeals on Security and Privacy Concerns

We hypothesized that there would be significant differences among groups regarding concerns about their smartphones' security and privacy and their use by other people (H2a), and that the customized group would have a higher level of concern about their smartphones' security and privacy and use by other people than would other treatment groups, which would be higher than that of the control group (H2b).

To test the hypotheses (H2a, H2b), we asked participants three questions related to their perceived vulnerability: "How much do you worry about your smartphone's security?", "How much do you worry about your smartphone's privacy?", and "How concerned are you about your smartphone use by others?" Answers regarding their worries and concerns were rated on a scale from (0) "Not at all" to (3) "Extremely."

We used the Kruskal-Wallis test to compare the five groups for those three questions, our results indicated that there were significant differences, with a significance level of $p \leq .001$ for the first question ($H(4) = 50.53$ with a large effect size, $\eta^2 = 0.25$), the second question ($H(4) = 55.47$ with a large effect size, $\eta^2 = 0.28$) and for the third question ($H(4) = 42.21$ with a large effect size, $\eta^2 = 0.21$).

As shown in Table 2 for the first question, we found significant differences for the first question when performing the Bonferroni multiple comparisons test with adjusted significance and mean rank. The percentages of participants who rated their concerns about their smartphone security as either "Moderately worried" or "Extremely worried" were as

"How much do you worry about your smartphones security?"	
Comparison of Groups (Mean Rank)	**Adj. Sig.**
Control (64.9) vs. Dubbed (127.4)	≤.001
Control (64.9) vs. Customized (135.7)	≤.001
Original (75.5) vs. Dubbed (127.4)	≤.001
Original (75.5) vs. Customized (135.7)	≤.001
Subtitled (98.9) vs. Customized (135.75)	.029
"How much do you worry about your smartphone's privacy?"	
Comparison of Groups (Mean Rank)	**Adj. Sig.**
Control (61.7) vs. Subtitled (99)	.026
Control (61.7) vs. Dubbed (126.3)	≤.001
Control (61.7) vs. Customized (139.2)	≤.001
Original (76.2) vs. Subtitled (99)	≤.001
Original (76.2) vs. Customized (139.2)	≤.001
Subtitled (99) vs. Customized (139.2)	.012
"How concerned are you about your smartphone being used by others?"	
Comparison of Groups (Mean Rank)	**Adj. Sig.**
Control (67.7) vs. Subtitled (106.6)	.019
Control (67.7) vs. Dubbed (116.3)	≤.001
Control (67.7) vs. Customized (136.6)	≤.001
Original (75.3) vs. Dubbed (116.3)	.010
Original (75.3) vs. Customized (136.6)	≤.001

Table 2: Post hoc test of the three questions on security and privacy concerns

follows: 75% of participants in the customized group (median = 2), 67.5% in the dubbed group (median = 2), 47% in the subtitled group (median = 1), 20% in the original group (median = 0), and 15% in the control group (median = 0).

For the second question about smartphone privacy, as shown in Table 2, we found significant differences between groups, as 47.5% of participants in the subtitled group (median = 1), 67.5% in the dubbed group (median = 2), and 75% in the customized group (median = 2.5) had moderate or extreme worries about their smartphone privacy, whereas 57.5% of participants in the original group (median = 0) and 65% in the control group (median = 0) chose "None at all."

When we asked participants a third question as to their concerns about others using their smartphones, we found significant differences between groups, as shown in Table 2. Percentages of participants who rated themselves as either "Moderately concerned" or "Extremely concerned" for each group were as follows: Customized, 82.5% (where median = 3); Dubbed, 67.5% (where median = 2); Subtitled, 57.5% (where median = 2); Original, 27.5% (where median = 1); and Control, 20% (where median = 1).

Thus, Hypotheses H2a and H2b were supported. The group that watched the customized video was more worried about their smartphones' security, privacy, and use by others than were other groups. Thus the video with customized content (Saudi identities, a Saudi bank, and fake dialogue to lure victims through WhatsApp messages) made participants aware of the risks of not using a screen lock on their smartphones.

5.5 Impact of Fear Appeals on Perceived Severity

For the third hypothesis (H3), we assumed that there would be significant differences among the groups' ratings of the perceived severity and risk awareness (H3a), and that the customized group would have higher ratings of the perceived severity and risk awareness than would the other treatment groups, which would be higher than those of the control group (H3b).

To test Hypothesis 3, we asked participants three questions. The first question was, "If your smartphone is lost or stolen, how disruptive will the loss of your data on your smartphone be to your daily life?" Participants rated their disruption from (0) "Not at all disruptive" to (3) "Highly disruptive." The second question was "How likely is it that you would lose your smartphone?" The third question was "How likely is it that someone else would attempt to access your smartphone?" For both questions, participants rated their likelihood on a scale from (0) "Extremely unlikely" to (3) "Extremely likely."

Performing the Kruskal-Wallis test, we found significant differences among the five groups for the three questions at a significance level of $\leq .001$ for the first question ($H(4) = 38.02$ with a large effect size, $\eta^2 = 0.19$), the second question ($H(4) = 26.31$ with a medium effect size, $\eta^2 = 0.13$) and for the third question ($H(4) = 28.92$ with a large effect size, $\eta^2 = 0.14$).

"If your smartphone is lost or stolen, how disruptive will the loss of your data on your smartphone be to your daily life?"	
Comparison of Groups (Mean Rank)	**Adj. Sig.**
Original (72.4) vs. Dubbed (121.8)	≤.001
Original (72.4) vs. Customized (134.8)	≤.001
Control (78.2) vs. Dubbed (121.8)	.005
Control (78.2) vs. Customized (134.8)	≤.001
Subtitled (95.2) vs. Customized (134.8)	.015
" How likely is it that you would lose your smartphone?"	
Comparison of Groups (Mean Rank)	**Adj. Sig.**
Control (75.7) vs. Dubbed (117.1)	.009
Control (75.7) vs. Customized (129)	≤.001
Original (82.2) vs. Customized (129)	.002
" How likely is it that someone else would attempt to access your smartphone?"	
Comparison of Groups (Mean Rank)	**Adj. Sig.**
Control (74.8) vs. Dubbed (115.6)	.011
Control (74.8) vs. Customized (131.9)	≤.001
Original (81.4) vs. Customized (131.9)	≤.001

Table 3: Post hoc test of the three questions on perceived severity

When we asked participants the first question, as shown in Table 3, we found significant differences between groups by performing the Bonferroni multiple comparisons test with adjusted significance and mean rank. A majority of participants in the dubbed group (median = 3) and the customized group (median = 3) indicated it would be highly disruptive, at 52.5% and 53.5%, respectively. In contrast, 17.5% of participants in the original group (median = 1), 32.5% in the subtitled group (median = 2), and 15% in the control group (median = 1) said it would be highly disruptive, which is significantly lower than in the customized and dubbed groups.

As shown in Table 3, for the second question, there were significant differences between the groups, as 37.5% of participants in the original group (median = 1) and 32.5% in the control group (median = 1) chose "Extremely unlikely", whereas 52.5% in the subtitled group chose "Moderate likely" (median = 2), 47.5% in the customized group (median = 2), and 45% in the dubbed group (median = 2) chose " Extremely likely."

For the third question, we found differences between the groups, as shown in Table 3. We noticed that 30% of the participants in the original group (median = 1.5) and 30% in the control group (median = 1) rated someone else's attempting to acces their phone " Extremely unlikely", whereas 50% in the dubbed group (median = 2.5), 50% in the customized group (median = 2.5) chose "Extremely likely", and 45% of the subtitled group (median = 2) chose "Moderate likely."

Thus, Hypotheses H3a and H3b were supported. The risk perceptions of both the subtitled and the original groups changed only minimally, perhaps because most of them did not pay attention to the Arabic captions or did not realize what the speaker was saying. In contrast, the assigned videos in the dubbed group and the customized group were extremely effective, and the impact was reflected in their perception of the seriousness of potential risks and possible adverse consequences of losing their personal information by not enabling a screen lock on their smartphones.

5.6 Impact of Fear Appeals on Response Cost

We hypothesized that there would be significant differences among the groups in their ratings of perceived response cost (H4a), and that the customized group would have lower ratings of perceived response cost than would other treatment groups, with the control group being the lowest (H4b).

To test Hypothesis 4, we asked participants whether they found using a screen lock to be a hassle, whether they agreed that entering an unlock code several times was inconvenient, and whether they agreed that it was inconvenient because a secure code was easily forgettable. We asked them to rate these on a scale ranging from (1) "Strongly disagree" to (5) "Strongly agree."

Performing the Kruskal-Wallis test, we found significant differences among all the groups for the first question ($H(4) = 24.76$, $p \leq .001$ with a medium effect size, $\eta^2 = 0.12$), the second question ($H(4) = 29.27$, $p \leq .001$ with a large effect size, $\eta^2 = 0.14$), and the third question ($H(4) = 17.55$, $p = .002$ with a medium effect size, $\eta^2 = 0.09$); therefore, H4a was supported.

The groups differed significantly, as shown in Table 4. Fewer participants from the dubbed group (median = 3) and the customized group (median = 3) agreed that the screen lock would be a hassle (25% and 27%, respectively), whereas in the original, subtitled, and control groups, 67.5%, 40%, and 55%, respectively, agreed that it would be a hassle.

For the second question, as shown in Table 4, we found significant differences between the groups, with 77.5% of participants in the original group (median = 5) agreeing it was inconvenient to enter a locking code, 65% in the subtitled group (median = 4), and 82.5% in the control group (median = 5). In contrast, both the dubbed (median = 2) and the customized groups (median = 2.5) had lower levels of agreement (40% and 45%, respectively).

"If I use a secure screen lock on my smartphone, it will be too much of a hassle for me"	
Comparison of Groups (Mean Rank)	**Adj. Sig.**
Customized (76.9) vs. Control (117.3)	.013
Customized (76.9) vs. Original (128.5)	≤.001
Dubbed (82.2) vs. Original (128.5)	.002
"I feel using a secure screen lock on my smartphone is too inconvenient due to having to enter an unlock code every time I use the phone "	
Comparison of Groups (Mean Rank)	**Adj. Sig.**
Dubbed (74.4) vs. Control (120.9)	.002
Dubbed (74.4) vs. Original (126.1)	≤.001
Customized (78.9) vs. Control (120.9)	.007
Customized (78.9) vs. Original (126.1)	≤.001
"I feel using a secure screen lock on my smartphone is too inconvenient because it is hard to remember"	
Comparison of Groups (Mean Rank)	**Adj. Sig.**
Customized (78.8) vs. Subtitled (114.5)	.043
Customized (78.8) vs. Control (118.9)	.013
Dubbed (82.7) vs. Control (118.9)	.037

Table 4: Post hoc test of the three questions on response cost

Differences were found between the groups in whether they thought it was too hard to remember a secure screen lock, as shown in Table 4. 42.5% of participants in the original group (median = 3) agreed with this idea, 40% in the subtitled group (median = 2.5), and 45% in the control group (median = 3). In contrast, only 22.5% of participants in the dubbed group (median = 2) and 20% in the customized group (median = 2) agreed with this, or about half as many.

Thus, Hypothesis 4 was supported; the evidence shows the major impact of effective risk communication: both dubbed and customized groups changed their perception of inconvenience (see section 5.2) and came to realize the importance of enabling a secure screen lock on their smartphones.

5.7 Impact of Fear Appeals on Response Efficacy

We assumed that there would be significant differences among the five groups in their ratings of response efficacy (H5a), and that the customized group would have higher ratings of response efficacy than would the other treatment groups, with the control group being lowest (H5b).

In this part, we measured participants' confidence in performing the recommended behavior of activating one of the screen lock methods and tested Hypothesis 5 by asking five questions. The first question was whether they thought that using a screen lock was a good idea. The second question was whether they thought it was easy to use it on their smartphones. The third question was whether they thought it secured their smartphones. The fourth question was whether they understood the purpose of using the screen lock. The last question was whether they thought a screen lock protected the data on their smartphones. Answers were rated using 5-point Likert scale from (1) = "Strongly disagree" to (5) = "Strongly agree."

Performing the Kruskal-Wallis test, we found differences among all groups at a significant level, $p \leq .001$, for the five questions (($H(4) = 48.26$ with a large effect size, $\eta^2 = 0.24$), ($H(4) = 47.37$ with a large effect size, $\eta^2 = 0.23$), ($H(4) = 51.66$ with a large effect size, $\eta^2 = 0.26$), ($H(4) = 56.87$ with a large effect size, $\eta^2 = 0.28$), and ($H(4) = 47.40$ with a large effect size, $\eta^2 = 0.24$), respectively).

"Do you think that using a screen lock is a good idea?"	
Comparison of Groups (Mean Rank)	**Adj. Sig.**
Control (69.6) vs. Dubbed (129.6)	≤.001
Control (69.6) vs. Customized (134.4)	≤.001
Original (71.5) vs. Dubbed (129.6)	≤.001
Original (71.5) vs. Customized (134.4)	≤.001
Subtitled (97.3) vs. Customized (134.4)	.031
"Do you think a screen lock is easy to use on your smartphone?"	
Comparison of Groups (Mean Rank)	**Adj. Sig.**
Original (69.7) vs. Customized (128.2)	≤.001
Original (69.7) vs. Dubbed (137.1)	≤.001
Control (74.3) vs. Customized (128.2)	≤.001
Control (74.3) vs. Dubbed (137.1)	≤.001
Subtitled (93.2) vs. Dubbed (137.1)	.005
"Do you think a screen lock secures your smartphone?"	
Comparison of Groups (Mean Rank)	**Adj. Sig.**
Control (66.9) vs. Dubbed (130.9)	≤.001
Control (66.9) vs. Customized (137.4)	≤.001
Original (78.9) vs. Dubbed (130.9)	≤.001
Original (78.9) vs. Customized (137.4)	≤.001
Subtitled (88.3) vs. Dubbed (130.9)	.006
Subtitled (88.3) vs. Customized (137.4)	≤.001
"Do you understand the purpose of using a screen lock?"	
Comparison of Groups (Mean Rank)	**Adj. Sig.**
Control (61.4) vs. Dubbed (132.2)	≤.001
Control (61.4) vs. Customized (137.1)	≤.001
Original (77.6) vs. Dubbed (132.2)	≤.001
Original (77.6) vs. Customized (137.1)	≤.001
Subtitled (94.2) vs. Dubbed (132.2)	.024
Subtitled (94.2) vs. Customized (137.1)	.006
"Do you think a screen lock protects your personal data in your smartphone?"	
Comparison of Groups (Mean Rank)	**Adj. Sig.**
Control (71.2) vs. Dubbed (130.3)	≤.001
Control (71.2) vs. Customized (136.2)	≤.001
Original (78.5) vs. Dubbed (130.3)	≤.001
Original (78.5) vs. Customized (136.2)	≤.001
Subtitled (86.3) vs. Dubbed (130.3)	.004
Subtitled (86.3) vs. Customized (136.2)	≤.001

Table 5: Post hoc test of the five questions on response efficacy

As shown in Table 5 for the first question, there were significant differences between the groups by performing the Bonferroni multiple comparisons test with adjusted significance and mean rank, as 77.5% of participants in the dubbed group (median = 5), 57.5% in the subtitled group (median = 4), and 82.5% in the customized group (median = 5) agreed with the first question, whereas only 35% of participants in the original group (median = 2) and 30% in the control group (median = 2) agreed, a level lower than the other groups.

We found significant differences between the groups for the second question, as shown in Table 5. 70% of participants in the original group (median = 2), 42.5% in the subtitled group (median = 3), and 65% in the control group (median = 2) thought that it would not be easy to use a screen lock, whereas 75% of participants in the dubbed group (median = 4) and 67.5% in the customized group (median = 4) thought that it would be easy to use.

As shown in Table 5, for the third question, there were significant differences among the groups. In the original (median = 3) and the control group (median = 3), 47.5% and 32.5%, respectively, agreed that the screen lock secured their smartphones, in contrast to 60% of participants in the subtitled group (median = 4), 82.5% in the dubbed group (median = 5), and 87.5% in the customized group (median = 5).

Significant differences were also found among the groups for the fourth question in Table 5. 82.5% of participants in the dubbed group (median = 5) and 87.5% in the customized group (median = 5) agreed that they understood the purpose of the screen lock, in contrast with 65% in the subtitled group (median = 4), 42.5% in the original group (median = 3), and 30% in the control group (median = 2).

Once again, we found significant differences among the groups for the last question in Table 5. 82.5% of participants in the dubbed group (median = 5) and 85% in the customized group (median = 5) agreed that a screen lock protected their data, in contrast to 60% in the subtitled group (median = 4), 47.5% of participants in the original group (median = 3), and 32% in the control group (median = 3).

These ratings supported the idea that the Saudi-customized video and the Arabic-dubbed video were significantly effective in raising participants' risk awareness and encouraging them to follow recommended security practices that would benefit them and changed their views about activating a secure screen lock.

5.8 Impact of Fear Appeals on Saudis' Behavior (Follow-Up)

A week after the initial interview; during the second round of the follow-up study, we contacted participants to see whether they had enabled the screen lock or not. We hypothesized that there would be significant differences among the groups in terms of the percentage of participants who enabled a screen lock (H6a), and that the customized group would have a higher level of participants who enabled a screen lock than the other treatment groups, with the control group being the lowest (H6b).

If participants answered " Yes", we asked them "What motivated you to enable it?", " When did you activate it?", "What is the type of the screen lock?", and " How was it?" If their answer was "No", we asked them to tell us their reasons for not employing the screen lock.

In this round, we tested our hypotheses to see who among the treatment groups and the control group had enabled the screen lock. As we had predicted in H6a, the KruskalWallis test ($H(4) = 39.46$, $p \leq .001$) indicated significant differences among the five groups in terms of the level of participants who enabled the screen locks.

As shown in Table 6, there were significant differences among the groups regarding the enabling of a screen lock. Table 7 shows the number of participants that did and did not enable a screen lock for all groups.

"Have you enabled the screen lock on your smartphone or not?"	
Comparison of Groups (Mean Rank)	**Adj. Sig.**
Control (75) vs. Dubbed (120)	≤.001
Control (75) vs. Customized (130)	≤.001
Original (77.5) vs. Dubbed (120)	≤.001
Original (77.5) vs. Customized (130)	≤.001

Table 6: Post hoc test of participants who did and did not enable a screen lock

Number of participants	**Enabled**	**Not enabled**
Original (n=40)	8	32
Dubbed (n=40)	25	15
Subtitled (n=40)	17	23
Customized (n=40)	29	11
Control (n=40)	7	33

Table 7: Number of participants who did and did not enable a screen lock for all groups

5.8.1 Comments from Those Enabling the Screen lock

When we asked participants about their motivation for enabling the screen lock, it revealed the thinking behind their responses. A participant from the original group said, " Graphics show the existence or truth of the meaning of not using screen lock, so I activated it in the same day after our interview." A participant from the dubbed group reported, "Now that I know the benefits of having a security code to protect my secrets, and I understand how hackers can steal my personal information from my online accounts. However, if the content in the video is written in Arabic, then it will be really clear, especially how to follow the steps of setting up a screen lock for anyone who does not know English. Of course, I activated the pattern on my phone." A participant from the subtitled group mentioned his motivations, saying, "The privacy examples in this video changed my mind about enabling a secure lock on my phone. I enabled it two days later because I was so busy after our interview." A participant in the customized group commented that "I became convinced of the risk that my data might get stolen if there was no screen lock. Most of my government transactions are managed by my husband. The most important documents are my bank records sent through WhatsApp messages, which includes my Saudi ID, my passport, and my bank information. Previously, I saw no risk from not locking the screen because my mobile was with me all the time, but after watching the video I learned a lot, and I will send this video to my acquaintances and friends. I activated a screen lock immediately after watching the video." A participant from the control group said, "I enabled the passcode again after I responded to the questionnaire. The questions made sense and led me to think about it again. After our interview, I enabled it immediately."

Most of the participants, who enabled screen locking mechanism, enabled it on the same day. Only six of our participants enabled it on the second day.

The control group stated as the first reason for their motivation that the questionnaire led them to change their locking behavior. Among the treatment groups, the main motivation for enabling the screen lock was the videos that they had watched: The numbers in parentheses indicate the number of participants who were motivated by that reason versus the total number of participants who had activated a screen lock for all motivations: Customized (23/29), Dubbed (22/25), Subtitled (13/17), Original (6/8), and Control (4/7). The second most commonly cited motivation was security and privacy concerns: Customized (4/29), Subtitled (3/17), Dubbed (2/25), Original (2/8), and Control (2/7). Only four participants out of all the groups stated having had a bad experience as a reason for their motivation.

Regarding the type of secure lock method used by members of all the groups, the most commonly used was passcode/Touch ID (35 participants), followed by pattern (22), PIN (18), fingerprint (17), and other secure]ity mechanisms (7). Overall, 58 participants said they found the use of a screen lock convenient, in contrast to the 27 who found it inconvenient.

5.8.2 Comments from Those Not Enabling the Screen Lock

Among the treatment groups and the control group, the stated reason for participants' not enabling a screen lock on their smartphones was " Forgettable" (28.9%), "Nothing to hide" (25%), "Annoying to use " (16.7%), "low perceived threat" (15.8%), "Don't know how to set up" (5.3%). The last chosen was "Another reason" (7.9%), meaning that participants stated a reason not listed, such as this one from the dubbed group: "I and my family use my phone as a personal hotspot for sharing Internet data, and it is annoying to put a screen lock on, especially when someone who trusts you shares your phone." A participant from the control group noted, "As there are some advanced tools that break the screen lock mechanisms, I am not motivated to use any of them."

5.9 Ratings for Treatment Groups

The present study investigated the effects of different video designs incorporating fear appeal on four treatment groups (160 participants). The results showed that communicating risk had a positive effect on peoples' perceptions which led them to change their screen locking behavior and increased their awareness of new security recommendations. The following section evaluates the video used for each treatment group (Customized, Dubbed, Subtitled, and Original).

As shown in Table 8, each treatment group of participants was shown their assigned video and were asked to rate the persuasion, believability, and effectiveness of the video on a scale from (0) "Not at all" to (3) "Very."

We noticed that the percentages of participants from the customized and the dubbed groups that found the video persuasive, believable, and effective, were higher than the percentages of participants who enabled the screen lock. The main reasons for the different percentages despite their high level of video rating, especially Customized and Dubbed, referred to their reasons for not employing the screen lock,

	Original	Dubbed	Subtitled	Customized
Enabled	20%	62.5%	42.5%	72.2%
Persuasion	17.5%	72.5%	35%	87.5%
Believability	10%	72%	47.5%	90%
Effectiveness	15%	82.5%	40%	92.5%

Table 8: Percentage of participants who enabled a screen lock and treatment groups' evaluations of videos

which were "Forgettable" (Customized : 36.4%, Dubbed: 40%) and "Nothing to hide" (Customized: 27.3%, Dubbed: 33.3%).

We asked participants in the treatment groups what aspects of the video they saw that they liked and did not like. Table 9 shows the good aspect and the bad aspect most chosen by participants in each group.

Spearman's coefficients were used to verify the correlation of a mutual relationship between participants' conviction that lock screen was a good idea and those who enabled it among treatment groups. Based on their responses, we found a significant correlation at $p \leq 0.001$, as shown in Table 10 (first row). We also verified the correlation of a mutual relationship of persuasive and effectiveness levels on the video with participants who enabled a screen lock on their smartphones at $p \leq 0.001$, as shown in Table 10 (second and third row, respectively). This showed the extent to which the video affects the participants, based on their assessment of the level of effectiveness and their conviction, that lead to change their locking behavior.

6. DISCUSSION

Through interviewing participants face to face, we were able to record their answers accurately, and we saw their reactions to the video reflected in their responses, especially for those in the treatment groups. It was interesting during our interview to listen to participants' questions related to our study that went beyond those in our questionnaire. For example, one of the participants from the customized group commented, "If the steps of setting up a screen lock were only printed on paper, it would be easy for people to follow the steps in case they did not watch the video."

The results of our study showed us that the Saudi customized-video had the most effect on participants' perceptions, and led them to change their phone-locking behavior. This can be attributed to the video customization, which employed banks that are heavily used in Saudi Arabia, an Arabic scenario in which the victim is deceived via the use of WhatsApp, and Arabic descriptions of how to enable a screen lock for both iOS and Android systems. The Arabic-dubbed video had the second highest level impact. These findings were based on the four axes set forth in the protection motivation theory [42]. In the second round, the follow-up study, depending on the impact of each video, the percentage of Saudi participants who employed the screen lock increased, to 72.5% for the customized group, to 62.5% for the dubbed group, to 42.5% for the subtitled group, and to 20% for the original group. This significant impact is reflected in participants' answers, especially those of the customized group and the dubbed group. Despite the impact of the videos on participants' locking behavior, however, 7 participants from the customized group and 11 participants from the dubbed group did not enable the screen lock, stating that the main reason they did not do so was either that the phone locking process was "Forgettable" or that they had "Nothing to hide."

Among the subtitled group, participants' responses to fear appeal questions varied. Our findings showed that this video was effective in a simple proportion. It was proven that the percentage of Saudi participants in the subtitled group who did not enable the screen lock was 57.5%, which was higher than the percentage of those who enabled it (42.5%). The extent of this simple effect was reflected in participants' answers. Those who did not enable the screen lock chose "Don't know how to set up a screen lock for iPhone" and "I did not understand the video's content." Participants who did not like the video's content complained that they did not understand the activation process because they focused on the video's graphics instead of on the Arabic captions.

Moreover, we found that the original video was only minimally effective in changing Saudis' locking behavior, as only 20% of our participants enabled their phone locks, compared 50% of the participants in the original study. It was clear from their responses that our treatment group who watched the original video had difficulties with the English dialogue, even though the graphics were simple. We noticed that responses from our original treatment group were very close to those of the control group, and we believe the reason was a lack of understanding of the video's content. Their comments also bear witness to the video's ineffectiveness; for example, "I trust all people around me who use my phone and I do not expect they will steal my personal information," and "Because of my age, I always forget what the password is and I do not know how to set up a screen lock." These can comments can be compared to those of participants from the control group, such as "I spend all my time using my phone, and it makes me so nervous each time I unlock my screen and the number of times I get confused especially in public places that I will not use it" and "As there are some advanced tools that break the screen lock, I am not motivated to use any screen lock mechanism."

Factors that participants identified as contributing to the effectiveness of a video and as making a positive impression were related to language, customized applications, and clearing up misconceptions about the purpose of phone locks. The factors are related to the perceptions that hindered them from enabling a screen lock on their smartphones. The last factor we noticed was misconceptions about the purpose of phone locks, which appeared clearly in participants' reasons for not locking the screen and their view of people using the locked screen before they had watched a video (Section 5.2).

7. LIMITATIONS AND FUTURE WORK

During our research before the first round of the main study, we faced several limitations. The hardest challenge we faced was the time required to search for participants who met the criteria in this study and to interview them individually. Additionally, the researcher recorded responses to the Arabic questionnaires that were given to participants, especially to the elderly.

Based on the sample numbers of the Saudi population, it is important to test for the age factor within the sample. For

Groups	Good aspect	Bad aspect
Original ($n = 40$)	Graphics (17/40)	Language (32/40)
Dubbed ($n = 40$)	Explanation of risks (21/40)	None (23/40)
Subtitled ($n = 40$)	Explanation of risks (13/40)	Language (22/40)
Customized ($n = 40$)	Explanation of risks (22/40)	None (37/40)

Table 9: Good and bad aspects of videos watched by treatment groups

	Original	Dubbed	Subtitled	Customized
Correlation between a screen lock as a good idea and those who enabled	.628 *	.701 *	.614 *	.803 *
Correlation between those who enabled and video persuasiveness	.665 *	.402 *	.714 *	.625 *
Correlation between those who enabled and video effectiveness	.662 *	.555 *	.617 *	.545 *

* Correlation is significant at .001

Table 10: Correlation of mutual relationship with behavior change among treatment groups

example, Alkhunaizan et al. [15] investigated the effects of mobile commerce acceptance among the Saudi population based on three factors: gender, age, and education. They found that the age factor significantly impacted mobile usage, indicating that further study of a larger sample in Saudi Arabia is needed to test the impact of age on the effectiveness of communicating risk to change behaviors.

Moreover, the native language of Saudis is Arabic; for example, when the original group and the subtitled group watched the video, most participants expressed that they did not understand the dialogue. However, some of them were able to understand via the graphics the consequences of not enabling screen lock. It is important to study social, cultural, and linguistic factors that motivate participants to change their behavior.

This study has proven the effectiveness of the customized video and the dubbed video in changing users' locking behavior andleading them to follow the recommended procedures to reduce risks. We found that, when we asked Saudi participants their initial reasons why people use a screen lock, the majority of their responses indicated they held a misconception about the reasons. After they watched the video, they changed their locking behavior. It is be good to conduct a similar study among the Saudi population dealing with cybercrime (e.g., blackmail) and to monitor the most important factors extracted from the data.

8. CONCLUSION

With the increase of cybercrime in Saudi Arabia, people have to be conscious of possible threats to their personal data if they do not follow security advice. We presented a replication of the study by Albayram et al. [14] on the Saudi population of smartphone users, and we extended the investigation of the effectiveness of several fear appeal video designs that fit Saudis' perceptions of locking behavior.

As a result of comparisons among the four treatment groups and the control group, we found that the most effective video among the treatment groups was the Saudi-customized video, as 72.5% of that group's participants enabled screen lock, and 92.5% rated this video as effective. The customized video included the Saudi-specific factors as described above in Section 4.1. The condition having the second-highest level of the effectiveness was the dubbed video, as 62.5% of that group's participants enabled their screen locks, and 82.5% rated this video as effective. After that came the original video with Arabic captions, as 42.5% of that group's participants enabled their screen locks, and 40% of them rated this video as effective. The least effective video was the original video for our Saudi original treatment group, as only 20% of that group's participants enabled their screen locks, and only 15% rated the video as effective, compared to the treatment group in the original study conducted in the U.S., where 50% of participants enabled their screen locks, In contrast, among the control group that was not shown any video, 17.5% enabled screen their locks, which was similar to the 21% who did so among the control group in the original U.S. study.

The participants' initial highest reason for not using their screen locks in all five groups was "Annoying to use" (30%); however, in the second round of the follow-up study, the highest-ranking reason changed to "Forgettable/Mental burden" (28.9%), but only for those who did not enable the screen lock on their smartphones. Finally, based on the impact of the fear appeal videos, the effectiveness of the Saudi-customized video showed that communicating risk had a significant effect on Saudis' perceptions that led them to change their locking behavior and to increase their awareness of the importance of following security recommendations.

9. ACKNOWLEDGMENTS

The authors express deepest gratitude to their families support. Special thanks to Dr. Heather Lipford for reviewing the study and providing feedback. Finally we would like to thank the Saudi participants for participating in this study.

10. REFERENCES

[1] 5 ways to protect your iphone from hackers. http://www.marketers-voice.com/2017/11/protect-your-iPhone-from-spyware.html. Accessed: 2018-02-08.

[2] Al rajhi bank: About us.

http://www.alrajhibank.com.sa/en/investor-relations/about-us/pages/about-us.aspx. Accessed: 2018-01-29.

[3] Cybercrime hit 6.5m in kingdom last year. http://www.arabnews.com/node/967966/saudi-arabia. Accessed: 2017-09-16.

[4] The head of the committees reveals and warns against responding to the demands of extortionists: most of them are sexual. https://sabq.org/GVKc5Y. Accessed: 2018-01-30.

[5] ICT Indicators in K.S.A by end Q2-2017. http://www.citc.gov.sa/en/reportsandstudies/indicators/Pages/CITCICTIndicators.aspx. Accessed: 2018-05-23.

[6] Interest in digital banking offers major opportunities for gulf banks. https://www.consultancy.uk/news/13440/interest-in-digital-banking-offers-major-opportunities-for-gulf-banks. Accessed: 2018-05-18.

[7] Kaspersky lab presents cybersecurity trends in the meta region. https://me-en.kaspersky.com/about/press-releases/2017_kaspersky-lab-presents-cybersecurity-trends-in-the-meta-region. Accessed: 2018-05-23.

[8] Mobile app ranking in saudi arabia. https://www.similarweb.com/apps/top/google/store-rank/sa/all/top-free. Accessed: 2018-01-24.

[9] The national center for cybersecurity. https://www.amen.sa/index.html. Accessed: 2018-05-24.

[10] Saudi arabia aims to develop cyber security, programming skills of students. http://english.alarabiya.net/en/variety/2018/02/04/Saudi-Arabia-aims-to-develop-cyber-security-skills-of-students-.html. Accessed: 2018-05-23.

[11] Saudi cyber security college signs mou for us training. http://www.arabnews.com/node/1291616/saudi-arabia. Accessed: 2018-05-23.

[12] Set the screen lock. https://support.google.com/nexus/answer/2819522?hl=ar. Accessed: 2018-02-08.

[13] Y. Albayram, M. M. H. Khan, and M. Fagan. A study on designing video tutorials for promoting security features: A case study in the context of two-factor authentication (2fa). *International Journal of Human–Computer Interaction*, pages 1–16, 2017.

[14] Y. Albayram, M. M. H. Khan, T. Jensen, and N. Nguyen. "... better to use a lock screen than to worry about saving a few seconds of time": Effect of fear appeal in the context of smartphone locking behavior. In *Symposium on Usable Privacy and Security (SOUPS)*, 2017.

[15] A. Alkhunaizan and S. Love. Effect of demography on mobile commerce frequency of actual use in saudi arabia. In *Advances in Information Systems and Technologies*, pages 125–131. Springer, 2013.

[16] A. Alzahrani and K. Alomar. Information security issues and threats in saudi arabia: A research survey. *International Journal of Computer Science Issues (IJCSI)*, 13(6):129, 2016.

[17] Anas. Five steps to protect your data from spyware, theft and loss on android. https://ardroid.com/5-steps-to-secure-your-android-phone/. Accessed: 2018-02-07.

[18] J. Blythe, J. Camp, and V. Garg. Targeted risk communication for computer security. In *Proceedings of the 16th International Conference on Intelligent User Interfaces*, pages 295–298. ACM, 2011.

[19] C. Bravo-Lillo, S. Komanduri, L. F. Cranor, R. W. Reeder, M. Sleeper, J. Downs, and S. Schechter. Your attention please: designing security-decision uis to make genuine risks harder to ignore. In *Proceedings of the Ninth Symposium on Usable Privacy and Security*, page 6. ACM, 2013.

[20] J. M. Clark and A. Paivio. Dual coding theory and education. *Educational Psychology Review*, 3(3):149–210, 1991.

[21] O. J. Dunn. Multiple comparisons among means. *Journal of the American Statistical Association*, 56(293):52–64, 1961.

[22] S. Egelman, M. Harbach, and E. Peer. Behavior ever follows intention: A validation of the security behavior intentions scale (sebis). In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, pages 5257–5261. ACM, 2016.

[23] S. Egelman, S. Jain, R. S. Portnoff, K. Liao, S. Consolvo, and D. Wagner. Are you ready to lock? In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, pages 750–761. ACM, 2014.

[24] A. Field. *Discovering statistics using IBM SPSS statistics*. Sage, 2013.

[25] V. Garg, L. J. Camp, K. Connelly, and L. Lorenzen-Huber. Risk communication design: Video vs. text. In *International Symposium on Privacy Enhancing Technologies Symposium*, pages 279–298. Springer, 2012.

[26] S. Gazette. Mobile banking, not traditional banking, is what saudi customers want: Infographic. https://www.albawaba.com/business/mobile-banking-saudi-arabia-infographic-1021314. Accessed: 2017-09-13.

[27] M. Harbach, A. De Luca, N. Malkin, and S. Egelman. Keep on lockin'in the free world: A multi-national comparison of smartphone locking. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, pages 4823–4827. ACM, 2016.

[28] M. Harbach, M. Hettig, S. Weber, and M. Smith. Using personal examples to improve risk communication for security & privacy decisions. In *Proceedings of the 32nd Annual ACM Conference on Human Factors in Computing Systems*, pages 2647–2656. ACM, 2014.

[29] M. Harbach, E. Von Zezschwitz, A. Fichtner, A. De Luca, and M. Smith. Itsa hard lock life: A field study of smartphone (un)locking behavior and risk perception. In *Symposium on Usable Privacy and Security (SOUPS)*, pages 9–11, 2014.

[30] C. Herron, H. York, C. Corrie, and S. P. Cole. A comparison study of the effects of a story-based video instructional package versus a text-based instructional package in the intermediate-level foreign language classroom. *Calico Journal*, pages 281–307, 2006.

[31] A. Jabir. What are the most significant risks faced by users? https://goo.gl/ti7y8L. Accessed: 2018-02-08.

[32] Y. Javed and M. Shehab. Investigating the animation of application permission dialogs: A case study of facebook. In *Data Privacy Management and Security Assurance*, pages 146–162. Springer, 2016.

[33] S. Kitayama, S. Duffy, T. Kawamura, and J. T. Larsen. Perceiving an object and its context in different cultures: A cultural look at new look. *Psychological Science*, 14(3):201–206, 2003.

[34] A. A. Madini and J. De Nooy. Cross-gender communication in a Saudi Arabian Internet discussion forum: Opportunities, attitudes, and reactions. *Convergence*, 22(1):54–70, 2016.

[35] P. Mayer, J. Kirchner, and M. Volkamer. A second look at password composition policies in the wild: Comparing samples from 2010 and 2016. In *Symposium on Usable Privacy and Security (SOUPS)*, 2017.

[36] I. Muslukhov, Y. Boshmaf, C. Kuo, J. Lester, and K. Beznosov. Understanding users' requirements for data protection in smartphones. In *Data Engineering Workshops (ICDEW), 2012 IEEE 28th International Conference*, pages 228–235. IEEE, 2012.

[37] I. Muslukhov, Y. Boshmaf, C. Kuo, J. Lester, and K. Beznosov. Know your enemy: the risk of unauthorized access in smartphones by insiders. In *Proceedings of the 15th International Conference on Human-Computer Interaction with Mobile Devices and Services*, pages 271–280. ACM, 2013.

[38] T. Nguyen and N. Memon. Smartwatches locking methods: A comparative study. In *Symposium on Usable Privacy and Security (SOUPS)*, 2017.

[39] A. Nishi, N. A. Christakis, and D. G. Rand. Cooperation, decision time, and culture: Online experiments with American and Indian participants. *PLOS ONE*, 12(2):e0171252, 2017.

[40] D. J. Ohana, L. Phillips, and L. Chen. Preventing cell phone intrusion and theft using biometrics. In *Security and Privacy Workshops (SPW), 2013 IEEE*, pages 173–180. IEEE, 2013.

[41] M. R. Pattinson and G. Anderson. How well are information risks being communicated to your computer end-users? *Information Management & Computer Security*, 15(5):362–371, 2007.

[42] R. W. Rogers. A protection motivation theory of fear appeals and attitude change1. *The Journal of Psychology*, 91(1):93–114, 1975.

[43] S. B. Salter and D. J. Sharp. Agency effects and escalation of commitment: do small national culture differences matter? *The International Journal of Accounting*, 36(1):33–45, 2001.

[44] A. Samer. 14 tips for protecting and securing mobile or tablet. https://mobilesgate.com/secure-android-mobile-top-ways/17956.php. Accessed: 2018-02-07.

[45] D. Van Bruggen, S. Liu, M. Kajzer, A. Striegel, C. R. Crowell, and J. D'Arcy. Modifying smartphone user locking behavior. In *Proceedings of the Ninth Symposium on Usable Privacy and Security*, page 10. ACM, 2013.

[46] C. D. Wetzel, P. H. Radtke, and H. W. Stern. *Instructional effectiveness of video media*. Lawrence Erlbaum Associates, Inc, 1994.

[47] K. Witte. Putting the fear back into fear appeals: The extended parallel process model. *Communications Monographs*, 59(4):329–349, 1992.

APPENDIX

A. CUSTOMIZED-VIDEO TRANSCRIPT

تم تصميم هذا الفيديو لشرح بعض المخاطر الرئيسية لعدم حماية جوالك وكيف تحمي نفسك من تلك المخاطر

كما تعلمون، الجوالات تخزن قدرا كبيرا من المعلومات الخاصة بك مثل بطاقة المصرف، محادثات الواتساب، رسائل البريد الإلكتروني، الفيديوهات والصور والمواقع، وبعض المعلومات الخاصة بك.

في حال تم سرقه او فقدان جوالك الذي لا يحتوي على أي رمز للقفل، يصبح من السهل جدا لشخص ما الوصول إلى البيانات المخزنة في جوالك.
صحيح! مجرد تخيل كم هو سهل بالنسبة لشخص ما التقاط الجوال الخاص بك والوصول إلى جميع المعلومات المخزنة في الجوال.

على سبيل المثال، إذا وقع جوالك في أيدي خاطئة، يمكن للمهاجم البحث بسهولة من خلال البريد الإلكتروني الخاص بك او الرسائل النصية لكلمة " بنك الراجحي " في حال اذا كنت تستخدم الخدمات المصرفية عبر الإنترنت او التطبيق المحمل في إجوالك فبتالي المهاجم يمكن ان ينقر زر الدخول لتلقى رساله نصيه من البنك في جوالك ويتم ادخال كلمه السر المؤقتة والتحكم في حسابك المصرفي.

إذا كان حساب بريدك الإلكتروني مرتبطا بالعديد من الحسابات الأخرى عبر الإنترنت، فيمكن للمهاجم استخدام نفس التقنية للتحكم في حساباتك الأخرى أيضا

بالإضافة، المهاجم يستطيع استكشاف المعلومات الحساسة الخاصة بك من خلال رسائل البريد الإلكتروني، مثل رقم الهوية ،جواز السفر والملفات المرفقة كسيره الذاتية ومعلومات بطاقات الائتمان للبنك وتاريخ الميلاد وكلمه المرور

إذا كان المهاجم يستطيع الحصول على هذه المعلومات كالهوية او جواز السفر فباستطاعته بيعها لصوص الهوية، أو انتحال شخصيتك بتقديم طلب للحصول على بطاقة ائتمان جديدة

إذا كان الهاتف يحتوي على صور لك أو لأهلك، يمكن للمهاجم استخدامها لابتزازك مقابل المال أو تدمير سمعتك عن طريق نشر .الصور على الانترنت أو إرسالها إلى جميع جهات الاتصال الخاصة بك

علاوة على ذالك، المهاجم بإمكانه استخدام بعض التطبيقات مثل الفيسبوك أو الواتساب لإرسال رسائل إلى أصدقائك أو غيرهم، يتظاهر بكونك انت ويسأل عن المال. بل يمكن أن يطلب منهم أن يأتوا إلى أماكن معينة كحالة طارئة

هذه الاحداث تسلط الضوء فقط على عدد قليل من المخاطر المشتركة الناتجة عن عدم قفل الجوال الخاص بك. فبتالي نستطيع تجنبها بسهولة باستخدام أي من آليات قفل الشاشة الأمنة المتاحة على الجوال الخاص بك مثل رمز الدخول، الرسم، كلمة المرور بشدة بها من قبل خبراء الأمن. هذه هي تدابير أمنية بسيطة لضمان عدم وصول أي شخص إلى أو بصمه الأصابع التي يوصى المحتويات المخزنة في جوالك دون إذنك

من السهل إعداد قفل الشاشة وعادة ما يستغرق أقل من دقيقة. ، على سبيل المثال لجوال الأفيون، يمكنك الانتقال إلى \ الاعدادات ثم اختيار البصمه ورمز الدخول |وبعدها يتم تفعيل قفل الشاشه

من ناحية انظمه الاندرويد الانتقال الى الاعدادات ثم اختيار خيار الامن ثم اختيار قفل الشاشة وبعدها يمكنك اختيار أي اليه لقفل الشاشة
أتمنى ان هذا الفيديو ساعدكم بادراك اهميه استخدام قفل الشاشة وتشجيعكم باستخدام اليه قفل الشاشة المتوفرة في جوالك
نشكركم على مشاهده الفيديو

B. ARABIC QUESTIONER

First Round of the Main Study
الدراسة الأساسية

Saudi background Questions (5 questions)

Q1) نوع الجنس
أ- ذكر
ب- انثى

Q2) كم عمرك بين هذه القيم
أ- اقل من ٢٠
ب- ٢٠-٢٩
ت- ٣٠-٣٩
ث- ٤٠-٤٩
ج- ٥٠-٥٩
ح- ٦٠-٦٩
خ- فوق ٧٠

Q3) مستوى التعليم
أ- امي (لا يقراء ولا يكتب)
ب- ابتدائية
ت- المتوسطة
ث- الثانوية
ج- جامعي
ح- ماجستير او دكتوراه

Q4) خلفيتك في استخدام الكومبيوتر
أ- لاشي
ب- منخفض
ت- وسط
ث- عالي

Q5) ماهي اللغة التي لديك
أ- العربي
ب- الانجليزي
ت- كلاهما

Saudi smartphone usage behavior Questions (5 questions)

Q1) ما هو نظام التشغيل المستخدم في جوالك؟
أ- IOS (الأيفون)
ب- Android (سامسونج)
ت- نظام اخر

Q2) يرجى تقدير عدد الساعات التي تستخدم الهاتف الذكي خلال اليوم
أ- 1-2 ساعتان
ب- 3-4 ساعات
ت- 5-6 ساعات
ث- أكثر من ست ساعات

Q3) كم عدد التطبيقات تم تنزيلها في جوالك
أ- 1-3 تطبيقات
ب- 4-6 تطبيقات
ت- أكثر من 6 تطبيقات
ث- لا يوجد

Q4) يرجى تقدير عدد الساعات التي يتم فيها استخدام تطبيقات الجوال (سناب شات، واتساب .....)
أ- 1-3 مرات
ب- 4-6 مرات
ت- أكثر من 6 مرات
ث- لا يوجد

Q5) ما تطبيقات التي تستخدمها يوميا
أ- واتساب
ب- فيسبوك، توتير
ت- سناب شات
ث- جميع التطبيقات
ج- تطبيقات اخرى

Online security behavior Questions (3 questions)

Q1) هل تشعر بالقلق في حاله تعرض حساباتك على الإنترنت للخطر أو الاستيلاء عليها
أ- نعم
ب- لا

Q2) هل تشعر بالقلق حول الامن باستخدامك الانترنت
أ- نعم
ب- لا

Q3) هل تستخدم برامج الحماية ضد الفايروسات في جوالك؟
أ- نعم
ب- لا

Reasons for Not Using Lock Screen (2 questions)

Q1) لماذا لا تستخدم احدى تقنيات قفل الشاشة لجوالك؟
أ- ليس لدي معرفه للإعدادات تفعيل قفل الشاشة
ب- لا توجد أي مخاطر
ت- لا يوجد شيء لإخفائه
ث- أنسى
ج- استخدام قفل الشاشة مزعج
ح- سبب اخر

Q2) برائيك، لماذا بعض الاشخاص يستخدمون احدى تقنيات قفل الشاشة لجوالاتهم؟

Video Evaluation (7 questions)

Q1) ما هو مستوى اقتناعك في هذا الفيديو؟
أ- غير مقنع
ب- نوعا ما مقنع
ت- مقنع بشكل متوسط
ث- مقنع بشده

Q2) ما هو مستوى المنطق في هذا الفيديو؟
أ- غير منطقي
ب- نوعا ما منطقي
ت- منطقي بشكل متوسط
ث- منطقي بشده

Q3) ما هو مستوى الفعالية في هذا الفيديو؟
أ- غير فعال
ب- نوعا ما فعال
ت- فعال بشكل متوسط
ث- فعال بشده

Q4) هل الفيديو جعلك مدرك للبيانات المخزنة في جوالك؟
أ- نعم
ب- لا

Q5) هل الفيديو جعلك قلق بخصوص امن وحماية جوالك؟
أ- نعم
ب- لا

Q6) ما لسمات التي عجبتك في هذا الفيديو؟
ت- اللغة
ث- شرح المخاطر
ج- المحتوى
ح- البساطة
خ- الصور
د- عرض طريقه استخدام قفل الشاشة
ذ- سبب اخر

Q7) ما لسمات التي لم تعجبك في هذا الفيديو؟
أ- لا شيء
ب- اللغه
ت- قله المعلومات
ث- المحتوى ممل
ج- المحتوى طويل
ح- الصور
خ- سبب اخر

Effect of Fear Appeal on Response Efficacy (5 questions)

Q1) استخدام شاشه القفل، سوف تكون فكره جيده
أ- (1) غير موافق بشده
ب- (2) غير موافق
ت- (3) عادي
ث- (4) موافق
ج- (5) موافق بشده

Q2) اعتقد ان شاشه القفل سهله الاستخدام
أ- (1) غير موافق بشده
ب- (2) غير موافق
ت- (3) عادي
ث- (4) موافق
ج- (5) موافق بشده

Q3) اعتقد ان تفعيل شاشه القفل، سوف يوفر الأمان لجوالي
أ- (1) غير موافق بشده
ب- (2) غير موافق
ت- (3) عادي
ث- (4) موافق
ج- (5) موافق بشده

Q4) فاهم ماهي فوائد استخدام شاشه القفل
أ- (1) غير موافق بشده
ب- (2) غير موافق
ت- (3) عادي
ث- (4) موافق
ج- (5) موافق بشده

Q5) اعتقد ان تفعيل شاشه القفل سوف يحمي بياناتي في جوالي
أ- (1) غير موافق بشده
ب- (2) غير موافق
ت- (3) عادي
ث- (4) موافق
ج- (5) موافق بشده

Second Round of the Follow up Study
الدراسة التاليه

Q1) هل فعلت رمز شاشه القفل لجوالك
أ- نعم
ب- لا

إذا الجواب نعم
Q2) ما لذي حمسك لتفعيل شاشه القفل على جوالك؟

أ- اهميه الأمان والخصوصية
ب- الفيديو
ت- تجربه سيئة
ث- أخرى

Q3) ما لذي حمسك لتفعيل شاشه القفل على جوالك ومتى فعلته ؟

Q4) ما هو نوع قفل الشاشه الذي تم تفعيله ؟

أ- البصمه
ب- الباسكود / البصمه للايفون
ت- الرمز السري لسامسونج
ث- النمط
ج- نوع اخر

Q5) كيف كان قفل الشاشة الذي تم تفعيله؟

أ- مريح
ب- غير مريح

إذا الإجابة لا
Q2) 2 لماذا لم تفعل شاشه القفل على جوالك؟

أ- انخفاض الادراك لتهديد
ب- استخدامه مزعج
ت- لا يوجد شيء لإخفائه
ث- ينسى
ج- عدم معرفه اعدادات تفعيل شاشة القفل
ح- سبب اخر

Effect of Fear Appeal on Perceived Data Value (2 questions)

Q1) هل تعتقد أن البيانات المخزنة على جوالك ذو قيمه لحمايته؟

أ- نعم
ب- لا

Q2) كم من البينات الخاصة والمهمة تخزنها في جوالك
أ- لا شيء على الإطلاق
ب- كميه منخفضة من المعلومات الخاصة
ت- كميه معتدلة من المعلومات الخاصة
ث- قدرا كبيرا من المعلومات الخاصة

Effect of Fear Appeal on Security and Privacy Concerns (3 questions)

Q1) ما هو مدى قلقك بشأن أمن الجوال الخاص بك؟
أ- (1) لست قلق على الإطلاق
ب- (2) نوعا ما قلق
ت- (3) بعض الأحيان قلق
ث- (4) قلق بشكل كبير

Q2) ما هو مدى قلقك بشأن خصوصيه الجوال الخاص بك؟
أ- (1) لست قلق على الإطلاق
ب- (2) نوعا ما قلق
ت- (3) بعض الأحيان قلق
ث- (4) قلق بشكل كبير

Q3) ما هو مدى قلقك بشأن استخدام الغرباء الجوال الخاص بك؟
أ- (1) لست قلق على الإطلاق
ب- (2) نوعا ما قلق
ت- (3) بعض الأحيان قلق
ث- (4) قلق بشكل كبير

Effect of Fear Appeal on perceived severity and risk awareness (3 questions)

Q1) ما هو مدى تأثير التدمير لفقدان او ضياع جوالك على حياتك اليومية؟
أ- (1) لا يوجد أي تأثير على الإطلاق
ب- (2) نوعا ما يوثر
ت- (3) بعض الأحيان يؤثر
ث- (4) يؤثر بشكل كبير

Q2) ما هو مدى احتمال فقدان جوالك؟
أ- (1) غير محتمل بشكل كبير
ب- (2) نوعا ما غير محتمل
ت- (3) نوعا ما محتمل
ث- (4) محتمل بشكل كبير

Q3) ما هو مدى احتمال وصول أي شخص لجوالك؟
أ- (1) غير محتمل بشكل كبير
ب- (2) نوعا ما غير محتمل
ت- (3) نوعا ما محتمل
ث- (4) محتمل بشكل كبير

Effect of Fear Appeal on Response Cost (3 questions)

Q1) في حال لو استخدمت شاشه القفل، سوف يكون صعب بنسبه لي
أ- (1) غير موافق بشده
ب- (2) غير موافق
ت- (3) عادي
ث- (4) موافق
ج- (5) موافق بشده

Q2) في حال لو استخدمت شاشه القفل، سوف يكون غير مريح في كل مره ادخل رمز القفل للجوال
أ- (1) غير موافق بشده
ب- (2) غير موافق
ت- (3) عادي
ث- (4) موافق
ج- (5) موافق بشده
من فضلك اشرح في جمل قصيره ما سبب اختيارك

Q3) في حال لو استخدمت شاشه القفل، سوف يكون غير مريح لصعوبة تذكر رمز القفل للجوال
أ- (1) غير موافق بشده
ب- (2) غير موافق
ت- (3) عادي
ث- (4) موافق
ج- (5) موافق بشده