Do Women in Conservative Societies (Not) Follow Smartphone Security Advice? A Case Study of Saudi Arabia and Pakistan

Elham Al Qahtani
UNC Charlotte
Charlotte, USA
ealqahta@uncc.edu

Yousra Javed
National University of Sciences & Technology
Islamabad, PK
yousra.javed@seecs.edu.pk

Heather Lipford
UNC Charlotte
Charlotte, USA
richter@uncc.edu

Mohamed Shehab
UNC Charlotte
Charlotte, USA
mshehab@uncc.edu

***Abstract*—Women in conservative cultures, are an understudied population when it comes to investigating how users keep their devices and data safe. Owing to the recent trend in smartphone adoption and the simultaneous increase in attacks targeting women in conservative societies, this study uses the rational decision model to investigate the motivations of this user group for (not) following common smartphone security advice. We focus on four pieces of smartphone security advice, i.e., using screen lock, updating device software, deleting suspicious text messages, and using secure WIFI networks. Through interviews with 156 women from Saudi Arabia and Pakistan, we re-validate the rational decision model, identify key gaps in perception between those who follow common smartphone security advice and those who do not, help explain participants' reasons behind their decisions and suggest recommendations for improving risk communication. Additionally, we describe similarities and differences between the studied population and the West in terms of sources for receiving smartphone security advice.**

***Index Terms*—mobile security advice, user study, women, conservative societies**

1. Introduction

Conservative cultures such as Pakistan and Saudi Arabia [9], assign a limited role for women in the wider society. Their customs include low participation of women in the workplace, women's prohibition from driving cars or practising Law and Engineering etc [11]. Women in these societies have also been less likely to own a phone compared to men [3], [4]. These numbers are even smaller for women not in the workforce (e.g., housewives and stay-home women) [4], [8], [36]. However, due to the mobile revolution, and the ubiquity and decrease in price of mobile phones, this user group is slowly witnessing a growth in smartphone ownership to be able to communicate with their family members and friends via phone calls and SMS. Other phone usage for this population includes social media (Facebook, WhatsApp etc) activity, Internet browsing, playing games, and watching shows [5], [22].

The growth in smartphone usage has simultaneously increased the prevalence of cybercrimes in conservative societies. Several of these attacks specifically target women. For instance, in Pakistan, women have been vulnerable to WhatsApp account hacking by gaining WhatsApp codes through phishing. The scammers claim to be from legitimate organisations, ranging from television game shows, the Pakistan Army, government departments such as the Benazir Welfare Programme and telecommunication companies [28]. To mitigate such threats, the Government of Pakistan has established the National Response Centre for Cybercrime (NRCC) and National Centre for Cybersecurity (NCCS) to create awareness among the masses [1], [2]. Similar bodies have also been set up in Saudi Arabia [6], [7].

Adopting common smartphone security measures is therefore recommended for protection against security and privacy attacks. These measures are often advertised through various mediums such as text messages, news, and websites and include such advice as 1) using a screen lock, 2) updating the device software, 3) deleting suspicious text messages, and 4) using a secure WIFI network [19], [37].

Since women (specifically those not in the workforce) in these societies have limited exposure to Cyber Security education and awareness on a daily basis, it is unclear to what extent these women are aware of smartphone security measures and follow them, and if so, what are their sources. Additionally, cybercrime aimed at women is increasing in both populations [28]. For these reasons, this paper investigates the motivations of women in conservative societies for following or not following smartphone security advice, and the sources from where they learn such advice. More specifically, we seek to answer the following research questions:

RQ1: Why do women in Saudi Arabia and Pakistan (not) follow smartphone security advice?

RQ2: What are the sources of smartphone security advice for women in these societies?

We conducted structured interviews with 156 women from two of the most conservative countries [9], namely, Saudi Arabia and Pakistan, due to their similarities in women's roles in the society. We based some of our questions off of the three-component (benefit, cost, and risk) rational decision model described by Fagan et al. in their 2016 SOUPS paper. Their study was conducted on the U.S. population for general computer security advice (e.g., update software, use a password manager, use 2FA, and change passwords). With these questions, we investigate our first research question as well as validate this model on 1) Saudi and Pakistani women population and 2) smartphone security advice (using a screen lock, updating the device software, deleting suspicious text messages, and using a secure WIFI network).

Our results show that there are differences in perceptions of women in conservative societies regarding the benefits, risks, and costs associated with their decisions. Both women who do and do not follow each advice report that their current decision regarding security advice gets them more benefit than if they changed. Those who follow the advice rate the risks of changing their decision as much higher than the risks reported by those who do not follow. Participants' reasoning for their decisions show strong trends highlighting the convenience/security trade-off. The major sources from whom our participants learn security advice include family/friends' past experiences, social media, Internet and Internet Service Providers (ISPs), and text messages, emails, and websites from the Government. Our findings suggest the need to address the divergence in women's perceptions using effective risk communication.

2. Rational Decision Model

Human beings use a rational model in their decision-making, i.e., they choose to minimize cost and/or maximize benefit. This equally applies to security decisions. Herley et al. [25] was the first to point out that users' failure to adhere to good security behaviors could be attributed to them finding the costs too high and/or benefits too low. They investigated how users make security decisions based on a rational decision model. Their findings suggest that the leading cause of (not) following the recommended security behavior is weighing the costs against the benefits for security actions, which impact the user's security decision (e.g., when a user rejects the security action due to the decision of weighing the cost that is too high and/or the benefit is too low).

Fagan et al. [20] separated "cost" into explicit cost/ inconvenience (e.g., time, money) and risk to provide a fuller picture of users' perceptions and motivations for (not) following security advice. The authors conducted a survey-based study on US participants via Mechanical Turk. The survey consisted of questions related to perceived benefit, cost, and risk of (not) following four pieces of computer security advice and the reasons for choosing to (not) follow this advice. The advice included updating software, using a password manager, using 2 Factor Authentication, and changing passwords. The participants were assigned to *Yes* or *No* groups for each computer security recommendation based on whether they followed that advice or not. Through quantitative and qualitative analysis, their findings showed differences in participants' perceptions of the rational choice as follows. Benefit perception – both groups perceived more benefits of their current decision than if they changed. Cost perception – the *Yes* group rated the cost of not following the advice higher than the *No* group, except for using 2FA. Risk perception – the *Yes* group perceived the risk of not following advice higher than the *No* group. Participants reported the security/convenience trade-off as the main reason for their decisions. This variation in people's perception of (not) following security measures explains a divergence in their decisions and behaviors. In this paper, we partially replicate this study by examining whether these results hold in a different population and with different advice.

3. Related Work

3.1. Cultural Context of Conservative Societies

Cultural expectations and social norms have a significant influence on a person's behavior in conservative societies. For example, both Saudi Arabia and Pakistan apply gender segregation in education, health, and mosques etc [31], [38].

Alruwaili et al. [16] studied how Saudi females identify themselves on social media in Saudi Arabia and the West. They found that females experienced more independence in their personality and were more open in expressing themselves through social media when they were studying in the U.S. Also, Abokhodair et al. [10] investigated how cultural norms impact the Arab gulf populations in representing themselves through online photo-sharing applications that reflect upon collectivism (e.g., with their families).

Sambasivan et al. [35] explored how cultural norms have influenced the shared phone usage in Pakistan, India, and Bangladesh. Families, especially women, share their device with husbands, parents, and children, which leads to privacy challenges. In another example, Alghamdi et al. [15] found that Saudi females share their bank credentials with their family members due to the trust and their perception of no risks from sharing. These studies covered implications for how women experience digital security and privacy, which can be influenced by their cultural norms. However, the literature on conservative societies (e.g., Saudi Arabia and Pakistan) is limited in its current form. We therefore contribute to this literature by focusing our study on this population.

3.2. Security Guidelines/Advice

Most existing studies on following security advice and guidelines have been conducted in the West. For example, Rick Wash [40] provided an explanation about which advice from computer security experts gets followed and which advice does not. Also, Ion et al. [27] found the security practices from experts (e.g., software update, password manager usage, 2FA usage) were not followed by non-experts.

Recently, Zou et al. [42] examined why users adopt and abandon expert advice on security, privacy, and identity theft protection practices. They found that the manual practices (e.g., checking the URL when visiting a website) and automated practices (e.g., using antivirus software) were more adopted compared to user interaction practices (e.g., using two-factor authentication). Also, practices were abandoned when users perceived high cost or inconvenience associated with performing them.

Regarding the motivations of following security-related measures, Egelman et al. [18] investigated why some users do not enable the lock screen on their smartphones and they found users underestimated the amount of sensitive data in their smartphones and consider inconvenience as their main reason. Vaniea et al. [39] explained the reasons why users do not install software updates. These reasons could be unawareness of the outcomes of an update, evaluating the value of an update, and the users' difficulties in understanding why an update is required.

In addition, users abandon future software updates due to a prior bad experience with updating [39]. In another study on the adoption of virtual private networks (VPNs), the authors discovered that privacy protection and fear of surveillance motivated users to adopt VPNs [32]. We extend this work by examining behaviors in securing smartphones. We focus on stayhome women since it is an underrepresented group in user studies.

3.3. Source of Security Information

Several studies have investigated the sources through which people in the West learn about computer security. The main sources include peoples' own personal experiences of facing problems and through educational training and awareness programs (e.g., phishing training) [14], [41]. Rader et al. [33] conducted an online survey about the sources of security related stories that participants learned. They found that family and friends were the major providers of negative security incidents in various contexts (e.g., scam, phishing, theft, breaking in, and PC security problems). These incidents subsequently impacted participants' security decisions.

Redmiles et al. [34] conducted semi-structured interviews to understand where and why users learn security advice. They found that participants learned from negative experiences that happened to themselves and security stories that are told by family, peers, or TV shows and movies. Some participants also learned from trusted resources such as IT colleagues in the workplace, IT friends, IT emails, service providers, or newsletters. The main reasons for accepting the security advice were trustworthiness and plausibility. In contrast, the reasons for security rejection were related to the frustration of the advice content, which could be marketing-oriented or difficult to understand.

Das et al. [17] investigated social influence (e.g., observing and learning from friends) on users' security behavior. Their findings show that conversations about security and privacy resulted after experiencing a negative data breach, observing others' insecure practices, and reading security related news articles. Moreover, Fennell et al. [21] found that narration of stories about the adoption of Two-factor authentication (2FA) were effective in motivating users to adopt 2FA. We expand upon this work by examining sources of security advice of a non-Western population.

4. Methodology

The Fagan et al. study [20] investigated the differences in motivations of US population for (not) following general computer security advice based on three components (benefits, costs, and risks). These components were measured between the users who follow and those who do not follow computer security advice (updating software, using a password manager, using two-factor authentication, and changing passwords frequently).

In this study, we use Fagan et al.'s methodology to investigate our first research question. However, we only focus on the individual concerns regarding the benefits, costs, and risks. The reason why we did not include questions about the social concerns for each decision was that the question's phrasing in Arabic and Urdu may bias participants who may think about individual concerns instead of social concerns. However, we use the rational decision choice and measured the weight of costs against the weight of benefits and negative risks for security advice toward individual's perceptions.

Our study includes quantitative and qualitative approaches to identify the motivations of Saudi and Pakistani women for (not) following smartphone security advice as well as the the sources of security measures in these populations. We focus on the following top four pieces of security advice for smartphones, taken from Avast and Symantec websites [19], [37]:

1) Using a screen lock
2) Updating the device's software
3) Deleting suspicious text messages
4) Using secure encrypted WIFI

For each piece of advice, we divide the participants into 2 groups:
Yes Group: participants who reported that they follow the security advice on their smartphones and
No Group: participants who reported that they do not follow the security advice.

We also asked participants the reason for their current decision towards each smartphone security advice and analyzed this qualitative data to understand the motivations behind their security decisions better. Secondly, participants were asked to rate their current decisions based on the benefit, risk, and cost for each advice. Additionally, both groups were asked open-ended questions about the sources from where they receive security advice.

4.1. RQ1 Hypotheses

We use the Fagan et al. hypotheses for measuring the components of rational decisions (benefit, risk, and cost) towards individual decisions based on the first research question "Why do some Saudi and Pakistani women follow smartphone security advice, whereas others do not?":

Hypothesis 1 (H1): There will be a difference between the Yes and No groups in their ratings for the benefits of (not) following the security advice. (H1a) The ratings for the benefits of following will be higher in the Yes group compared to the No group. (H1b) The ratings for the benefits of not following will be higher in the No group compared to the Yes group.

Hypothesis 2 (H2): There will be a difference between the Yes and No groups in their ratings for the risks of (not) following the security advice. (H2a) The ratings for the risks of following will be higher in the No group compared to the Yes group. (H2b) The ratings for the risks of not following will be higher in the Yes group compared to the No group.

Hypothesis 3 (H3): There will be a difference between Yes and No groups in their ratings for the cost of (not) following the security advice. (H3a) The ratings for the cost of following will be higher in the No group compared to the Yes group. (H3b) The ratings for the cost of not following will be higher in the Yes group compared to the No group.

4.2. Study Design

The original study [20] focused on U.S. participants via MTurk. In contrast, we used in-person interviews with women from Saudi Arabia and Pakistan due to the unavailability of online crowdsourcing platforms such as MTurk in these countries. The two first authors, who are female, conducted the interviews in a public or private space depending on where the participants were recruited. The interview comprised of a mix of survey style questions to quantify participant behavior, followed by open-ended questions to inquire about the rationale for this behavior and sources for receiving smartphone security advice. No audio was recorded during the interview. The interviewer took notes and stored the responses in a spreadsheet. Participants provided their language preference for the interview; i.e., Arabic or English for Saudis and Urdu or English for Pakistanis. The study was approved by the Institution's Review Board [Protocol#19-0218], and took approximately 25 minutes to complete.

The participants first read and agreed to the consent form to be a part of the study. Each participant first answered demographic questions (such as nationality, age, and education level), smartphone usage, and security expertise questions.

The next set of questions were used to place the participant in the Yes or No group for each piece of security advice. For each piece of advice, they then answered questions regarding the reasons for (not) following the security advice and the perceived benefit, cost, and risk.

Lastly, the participants were asked about their source of smartphone security advice. At the end, we thanked each participant for their time and answered any further questions they had. The interview questions were translated to Arabic and Urdu by the authors.

4.3. Sampling Method

We recruited women from Abha and Dammam (Saudi Arabia), and Islamabad (Pakistan). The eligibility criteria was as follows: the participant must be a resident of one of these two countries, own a smartphone, stay at home or work from home, and is not a student. To recruit these women, we used a mix of convenience and snowball sampling. Most of the participants were recruited from women's public gathering places (such as female gyms, shops etc). The interviewers went up to these women in-person and asked to see if they are interested and met our criteria. A few of the participants were recruited from friends/relatives homes by visiting them. We requested the participants to spread the word about our study to eligible women. The participation was voluntary and no incentive was provided. However, each participant was debriefed about the goals of the study and how their data will help in our research.

4.4. Analysis Method

We collected both quantitative and qualitative data. Our quantitative data for both population (Saudia Arabia and Pakistan) was not normally distributed. Therefore, we used the Mann-Whitney U-test for analyzing the difference between the Yes and No groups for both samples separately. Moreover, we leveraged a 5-point Likert scale for the benefit, risk, and cost rating questions for each of the four smartphone security measures (0 = None, 1 = Not sure, 2 = little, 3 = Some, and 4 = A lot). We utilized SPSS for quantitative data analysis.

For analyzing qualitative data, we translated it back to English and utilized an inductive approach. Two researchers coded the data independently. These two set of codes were then discussed, refined, and updated to resolve any disagreements. Cohen's Kappa was used to test the reliability. We found k= .9 at $p<.001$.

5. Evaluation

We interviewed 156 stay-home women: 102 from Saudi Arabia (SA) and 54 from Pakistan (PK). 24.5% and 44.4% of the participants were between the ages 20-29, 35% and 13% between the ages 30-39, and 23.5% and 26% between the ages 40-49 from SA and PK, respectively. Our sample was relatively educated, as the majority of the Saudi and Pakistani participants had a bachelor's degree (62% and 52%, respectively) and frequently used a smartphone (74.6% and 79.6%, respectively).

Table 1 shows the participant responses for (not) following each of the four pieces of smartphone security advice in Saudi Arabia (SA) and Pakistan (PK). This resulted in 8 groups, i.e., 1 Yes and 1 No group per security advice.

TABLE 1. RESPONSES (PERCENTAGES) FROM SAUDI PARTICIPANTS **SA** (N=102) AND PAKISTANI PARTICIPANTS **PK** (N=54)

Security Advice	**Yes** SA,PK	**No** SA,PK	**Don't Know** SA,PK
Do you use screen lock/passcode on your smartphone?	92, 41 (90%, 76%)	10, 13 (10%, 24%)	0,0 (0%,0%)
Do you update your smartphone (install software updates)?	82, 31 (80%, 57%)	18, 12 (17%, 22%)	2,11 (2%, 20%)
Do you delete suspicious text messages from your smartphone?	72, 27 (70%, 50%)	24, 23 (23%,43%)	6,4 (5%,7%)
Do you always use secure WIFI for Internet on your smartphone?	67, 23 (65%, 43%)	31, 21 (30%, 39 %)	4, 10 (4%, 18%)

5.1. Differences in Perceptions

To test our hypotheses (Section 4.1), we compared the perceived weight of costs against the weight of benefits and negative risks between the Yes group who complies with smartphone security advice and the No group, who does not follow smartphone security advice. These three components (cost, benefit, risk) of the rational decision model were measured on a 5-point Likert scale for each of the four pieces of smartphone security advice (0 = None, 1 = Not sure, 2 = little, 3 = Some, and 4 = A lot).

We asked repetitive questions for the benefit, risk, and cost of following each of the four security advice. To test H1a, H2a, and H3a for both populations independently, the Yes group participants were asked *"How much would you say* ***(you have benefited by)*** *or* ***(you are put at risk by)****: 1) using a screen lock, 2) updating the device's software, 3) deleting suspicious text messages,*

and 4) using secure WIFI?" and for the cost, *"How much would you say you **would be inconvenienced** if you did not: 1) use a screen lock, 2) update device's software, 3) delete suspicious text messages, and 4) use secure WIFI?"*. Whereas, the No group participants were asked *"How much would you say **(you would benefit)** or **(you would be put at risk)** if you did: use a screen lock, update device's software, delete suspicious text messages, and use secure encrypted WIFI?"* and for the cost, *"How much would you say **you are inconvenienced** by not: 1) using a screen lock, 2) updating device's software, 3) deleting suspicious text messages, and 4) using secure WIFI?"*

Also, to test H1b, H2b, and H3b for each population, we asked the Yes group participants *"How much would you say **(you would benefit)**, **(you would be put at risk)** or **(you would be inconvenienced)** if you did not: 1) use a screen lock, 2) update the device's software, 3) delete suspicious text messages, and 4) use secure encrypted WIFI?"* Whereas, the No group participants were asked *"How much would you say **(you would benefit)**, **(you would be put at risk)** or **(you would be inconvenienced)** by not: 1) using a screen lock, 2) updating the device's software, 3) deleting suspicious text messages, and 4) using secure encrypted WIFI?"* The responses for all security advice were measured on a Likert scale ranging from "None" to "A lot."

5.1.1. Perception of Benefit. Regarding H1a, the U-test showed that the benefit of following a piece of security advice was rated significantly higher by the Yes group compared to the No group (See Table 2), except the WIFI usage that was rated by Pakistani participants. Therefore, Saudi and Pakistani participants from the Yes group felt that they benefited a lot from following the majority of security advice measures compared to the No group.

TABLE 2. THE BENEFIT OF FOLLOWING AND NOT FOLLOWING EACH SECURITY ADVICE BETWEEN YES AND NO GROUPS FOR BOTH POPULATIONS SA AND PK

	Security Advice		Yes Grp Mean	No Grp Mean	U-test	Sig.
Benefit of Following	**Lock Usage**	SA	3.8	2.1	226	**<.001**
		PK	3.3	1.5	87.5	**<.001**
	Update	SA	3.6	2.6	433.5	**<.001**
		PK	2.6	1.7	112.5	**.060**
	Deletion	SA	3.5	2.2	441.5	**<.001**
		PK	2.3	1.4	204.5	**.033**
	WIFI Usage	SA	3.5	3.1	766	**.013**
		PK	3.0	2.5	181.5	.134
Benefit of Not Following	**Lock Usage**	SA	1.1	2.2	340	**.024**
		PK	1.5	2.5	166.5	**.037**
	Update	SA	1.2	1.2	732	.88
		PK	1.2	2.1	119.5	.09
	Deletion	SA	1.3	1.3	869	.95
		PK	0.8	1.4	214	.05
	WIFI Usage	SA	1.8	2.9	634.5	**.002**
		PK	1.2	2.0	159.5	**.043**

Regarding H1b, the U-test showed that the No group Saudi and Pakistani participants felt they benefited significantly more from not using the screen lock and secure WIFI compared to the Yes group participants (See Table 2). However, for both populations, there was no significant difference in the responses for updating smartphone software and deleting suspicious text messages. The participants' reasons for providing these ratings are presented in section 5.2.

H1a is supported for all security advice, except the WIFI usage for Pakistani participants. Unsurprisingly, the Yes group participants valued the benefit of acting upon the most recommended smartphone measures compared to the No group participants, confirming the Fagan study. However, H1b is supported only for some security measures. The No group participants for both populations perceived the benefit of not using a screen lock and not using secure WIFI more than the Yes group participants, but did not perceive that benefit for updates and deleting suspicious text messages.

5.1.2. Perception of Risk. Regarding H2a, we did not find any statistically significant differences between the two groups' ratings for the risk of following each smartphone security advice in SA and PK, except the screen lock usage in SA (see Table 3). Thus there is low perceived risk overall, as both groups understand that following a security measure does not cause any new security issues.

TABLE 3. THE RISK OF FOLLOWING AND NOT FOLLOWING EACH SECURITY ADVICE BETWEEN YES AND NO GROUPS FOR BOTH POPULATIONS SA AND PK

	Security Advice		Yes Grp Mean	No Grp Mean	U-test	Sig.
Risk of Following	**Lock Usage**	SA	1.6	0.5	330.5	**.023**
		PK	0.9	1.4	1059	.142
	Update	SA	1.5	2.1	569.5	.104
		PK	0.9	1.7	135.5	.219
	Deletion	SA	1.3	0.9	760.5	.304
		PK	1.0	1.1	286	.612
	WIFI Usage	SA	1.5	1.3	960.5	.532
		PK	1.0	1.2	218.5	.564
Risk of Not Following	**Lock Usage**	SA	2.9	1.4	270	**.003**
		PK	3.2	1.3	83.5	**<.001**
	Update	SA	2.2	1.0	406	**.002**
		PK	3.37	2.88	1696.5	**.002**
	Deletion	SA	1.8	0.8	541.5	**.004**
		PK	2.2	1.3	191	**.017**
	WIFI Usage	SA	2.4	1.6	727.5	**.015**
		PK	2.6	2.1	190.5	.217

Regarding H2b, the results (see Table 3) showed that participants from the Yes group rated the risks of not following all security advice significantly higher than the No group. The Yes group understands that the probability of negative consequences happening are higher if they do not adhere to the security measures. However, we did not find a significant difference between the Yes and No PK groups for the risk of not using secure WIFI.

Hypothesis H2b is supported, except the risk of not using secure WIFI in PK. Participants in SA and PK from the Yes group rated the risks higher than the No group if they stopped following the security advice. On the other hand, both groups perceived that no risks would happen when they follow all security measures.

5.1.3. Perception of Cost. Regarding H3a, the results (Table 4) showed that the No group rated the cost of using the screen lock in SA and PK, updating the software in PK, and deleting suspicious texts in PK significantly higher than the Yes group. For the remaining advice,

although on average, the No group rated the cost of following as higher than the Yes group, the differences were not significant.

Regarding H3b, the results are shown in Table 4. We found that participants from the Yes group rated the cost of not using a screen lock in SA and PK, updating the device's software in SA, deleting suspicious text messages in PK, and using secure encrypted WIFI in SA significantly higher than the No group. For the remaining advice, although on average, the Yes group rated the cost of not following as higher than the No group, the differences were not significant. Details regarding the reasons for these ratings are presented in Section 5.2.

Both hypotheses are supported for some security advice (see Table 4). Results showed that participants in SA and PK from the Yes group rated the cost of not following some advice higher that of the No group. Based on the results, the Yes group's perception about convenience associated with following these security advice measures affected their rational security decisions.

Table 5 summarizes the results of the hypotheses regarding perceptions of benefit, risk, and cost of (not) following smartphone security advice.

TABLE 4. THE INCONVENIENCE OF FOLLOWING AND NOT FOLLOWING EACH SECURITY ADVICE BETWEEN YES AND NO GROUPS FOR BOTH POPULATIONS SA AND PK

	Security Advice		Yes Grp Mean	No Grp Mean	U-test	Sig.
Cost of Following	Lock Usage	SA	1.0	1.6	459	**.023**
		PK	1.5	2.4	163	**.031**
	Update	SA	1.5	2.0	601	.17
		PK	1.5	2.7	82.5	**.005**
	Deletion	SA	1.0	1.0	839.5	.731
		PK	1.4	2.5	177	**.008**
	WIFI Usage	SA	1.5	1.9	861.5	.159
		PK	1.4	1.7	205	.376
Cost of Not Following	Lock Usage	SA	2.7	1.5	326	**.020**
		PK	2.3	1.0	135	**.006**
	Update	SA	2.2	1.3	485.5	**.018**
		PK	2.3	2.0	159	.57
	Deletion	SA	2.2	1.5	648.5	.051
		PK	2.0	1.2	208	**.040**
	WIFI Usage	SA	2.3	1.6	730	**.016**
		PK	1.8	1.4	199.5	.308

TABLE 5. HYPOTHESES RESULTS SUMMARY

Hypothesis	Supported	Not Supported	Partial Support
H1a: Benefit ratings of following is higher for Yes grp vs No grp	✓		
H1b: Benefit ratings of not following is higher for No grp vs Yes grp			✓
H2a: Risk ratings of following is higher for No grp vs Yes grp		✓	
H2b: Risk ratings of not following is higher for Yes grp vs No grp	✓		
H3a: Cost ratings of following is higher for No grp vs Yes grp			✓
H3b: Cost ratings of not following is higher for Yes grp vs No grp			✓

5.2. Reasons for (Not) Following Smartphone Security Advice

In the previous section, we provided our findings regarding the differences in participant perceptions of cost, benefit, and risk to understand why some Saudi and Pakistani women follow smartphone security advice, whereas others do not. In order to better understand the perceived differences between the Yes and No groups, it is essential to understand the reasons why our participants chose to follow or not follow a particular piece of security advice. We, therefore, asked our participants a series of open-ended questions and used an inductive approach on the resulting qualitative data. The coding procedures were described in Section 4.4. Below, we report the main codes derived from participants' responses.

5.2.1. Using a Screen Lock. The first layer of access control on a smartphone is a screen lock (e.g., PIN, pattern, fingerprint, and face recognition). Without using a screen lock, anyone can easily access the personal data and apps stored in the smartphone. Enabling a screen lock ensures access control but can be inconvenient for users, especially if they share phones.

We asked our Yes group participants *"Why do you choose to use a screen lock on your smartphone?"* whereas, the No group participants were asked *"Why do you choose to not use a screen lock on your smartphone?"*. The participants answered these questions before they reported their perceptions of the benefit, risk, and cost of (not) following each security advice.

Access Control. 39.1% (SA) and 53.6% (PK) of the Yes group participants use screen lock to prevent kids from playing with the phone and damaging it, as well as to prevent outsider access.

Data Protection. 33.7% (SA) and 56% (PK) of the Yes group participants use screen lock to protect personal data in their smartphones (e.g., photos, videos, and notes). Some participant comments are as follows: *"To keep my data secure if my phone ever gets lost or stolen"*, and *"To secure my social media account especially my Facebook, to secure my Facebook chat with others."*

Privacy. 29.3% (SA) and 17% (PK) of the Yes group participants use screen lock for privacy purposes as some of them stated,*"So I can guarantee privacy, and that no one opens my mobile"*, and *"To hide my messages"*.

On the other hand, amongst the No group participants, inconvenience and risk underestimation were the key reasons for why they do not use a screen lock on their smartphones.

Inconvenience. Our findings confirm other studies [12], [18], [24] that inconvenience was the primary reason for users to not enable the screen lock on their smartphones. 20% (SA) and 23% (PK) of the No group participants do not enable the screen lock due to the inconvenience that results from their kids playing with the lock screen and inadvertently causing more problems.

Not important. Perceiving the presence of a screen lock might not be valuable due to underestimation of the possible risk that may happen to the smartphones and the amount of sensitive data inside their smartphones. 40% (SA) and 23% (PK) of the No group participants stated that the reason they do not use a screen lock is that it is not vital to lock their device.

Nothing to hide. Participants underestimated the importance of the data stored on their smartphones (e.g., their online accounts, messaging apps, and email accounts) and believed that only a specific type of data should be

protected (e.g., family photos). 10% (SA) and 38.4% (PK) of the No group participants mentioned that they have nothing to hide in their smartphones.

One interesting finding here is that some Yes group participants perceived that the presence of a screen lock will prevent their kids from accessing their smartphones, whereas some No group participants did not enable screen lock to prevent their kids from playing with the screen lock (e.g., pattern unlock) and causing more problems.

5.2.2. Updating the Smartphone Software. A vital security measure in a smartphone is regularly updating the operating system to the latest version. With regular software updates, new bugs and vulnerabilities are patched, thus securing the device.

We asked the Yes group participants *"Why do you choose to update your smartphones' software?"* whereas, the No group participants were asked *"Why do you choose to not update your smartphone's software?"*

Getting new features and improving the security performance were the key reasons for why our participants chose to update their smartphones' software.

Improving Performance and Security. 52% (SA) and 58% (PK) of the Yes group participants were aware that the smartphone updates help fix bugs, and patch vulnerabilities. One participant commented: *"I install software updates because they are useful and keep things running smoothly. It improves smartphone user experience and ensures everything is up to date"*

New Features. 35% (SA) and 54% (PK) of the Yes group participants reported that the main reason they update their smartphone's OS is to get new features.

On the contrary, amongst the No group participants, cost was the key reason for why they do not update the software of their smartphones.

Difficulty in Updating. Many of our participants, 33.3% (SA) and 25% (PK) of the No group participants mentioned that the reason for not updating is the difficulty in realizing the purpose of the update as well as understanding the update procedure.

Time-consuming. Also, 11% (SA) and 25% (PK) of the No group participants reported that a software update is time-consuming, and thus they have not considered it.

So, the notable reasons we found for the No group participants for not updating the software were their lack of knowledge about software updates, i.e., understanding the update process and its purpose. Whereas the Yes group participants valued the new features that come with updates along with improved performance and security.

5.2.3. Deleting Suspicious Text Messages. Deleting unsolicited and suspicious text messages from unknown sources is recommended by security experts. These messages often ask people to click on a malicious link or respond/call for providing important information related to user's personal accounts.

We asked the Yes group participants *"Why do you choose to delete suspicious text messages in the smartphone?"* whereas, the No group participants were asked *"Why do you choose to not delete suspicious text messages in the smartphone?"*

Amongst the Yes group participants, smartphone/data protection, and freeing up space from unwanted messages were the key reasons for deleting suspicious text messages from the smartphone.

Smartphone/data Protection. 44% of the Saudi and Pakistani participants reported protection against malware, attack, or data theft as the main reasons for suspicious text deletion. One participant said that she started deleting suspicious messages after she had a terrible experience. She commented, *"I often fall victim to fake messages pretending to be from my bank, etc. and have to ask family members to confirm if they are genuine. One instance is a fake message that I received from HBL bank. Luckily, I didn't know how to send them my details, so I asked my son to send them my details, and he stopped me."* Another comment was, *"Because it may contain a virus that harms the device and its existing data."*

Unwanted. 36% (SA) and 29.6% (PK) of the Yes group participants follow this security advice because these messages are not essential and come from unknown people. One participant stated: *"I don't like to keep messages from unknown numbers in my phone as there is a possibility of someone hacking my phone."*

Storage Space Consumption. 5.5% (SA) and 29.6% (PK) of the Yes group participants mentioned their reason as storage space consumption. One participant commented: *"Deleting these messages, frees up a lot of space on the phone."*

On the other hand, amongst the participants who do not delete suspicious text messages, a lack of need and perceived risks were the key reasons.

Do not care. We found that 62.5% (SA) and 30.4% (PK) of the No group participants do not care about such messages, and they do not delete them from their phone. Comments include *"I just see them and ignore them, I have no memory/space issue, so I don't delete."*

No Risks. Also, 8.3% (SA) and 39% (PK) of the No group participants perceived that there are no risks from not deleting suspicious text messages.

Time Consuming. 8.3% (SA) and 21.7% (PK) of the participants stated that it is time-consuming and inconvenient delete these messages often.

We noticed that the Yes and No groups have different perceptions regarding (not) deleting suspicious text messages. For example, the yes group stated security reasons and that the messages from unwanted sources are annoying, and they take up space in the memory. On the other hand, time-consumption (takes too much time to report and remove) and no involved risks associated with unwanted messages were reported by the No group.

5.2.4. Using Secure WIFI. It is important to use a password-protected and encrypted WIFI network to ensure security and privacy. Connecting to public and unencrypted WiFi networks will open doors for hackers to steal users' personal and financial information and put their smartphone security at risk. If using public WIFI, it is recommended to use a VPN to protect identity and secure online communication.

We asked the Yes group participants *"Why do you choose to use secure WIFI networks on a smartphone?"*. Whereas, the No group participants were asked *"Why do you choose to not use secure WIFI networks on a smartphone?"*

Security purposes was the key participant motivation for why they use secure WIFI networks on a smartphone.

Security. A majority of the Yes group participants, 59.7% (SA) and 65% (PK), mentioned using secure encrypted WIFI for safety, data protection, and access control as the major reasons for following this advice. One comment related to this reason was, *"I use encrypted and password protected WIFI networks because open public networks are not safe to use. As anyone else using the network can see all the data moving over them"*.

Availability. 12% (SA) and 30% (PK) of the Yes group participants mentioned that they only use the secure WIFI available at their home since they spend most of their time at home. One participant commented: *"My son set up my phone to use home WiFi, outside I use mobile data package, so its all taken care of"*.

In contrast, participants' need to use Internet, ease of access to free WIFI, and low risks were the key reasons for participants' who do not use secure WIFI networks on their smartphone.

Internet Need. 54.8% (SA) and 28.5% (PK) of the No group participants reported their urgent need for the Internet. One of the participants commented, *"Because if I need WiFi, then I don't mind if they are open."*

Ease of Access. 19% (SA) and 62% (PK) of the No group participants stated that the reason for connecting to unsecure WIFI is its ease of access and free of cost. Participants commented *"Free and I can register quickly without typing the password"*, and *"Its easily available and convenient whenever I am outside."*

Low Risks. A few participants, 3.2% (SA) and 14.2% (PK) respectively, mentioned that the risks of using free WIFI are low. One participant stated: *"I don't think anyone is sitting at public spaces waiting to hack me."*

The participant responses show that the current behavior of the Yes and No groups regarding using secure WIFI do not overlap. None of the participants mentioned using a VPN while connecting to the public WIFI in both groups. The majority of the No group participants use the public WIFI due to the convenience and low cost. On the other hand, the Yes group expressed security and privacy concerns and mostly use the secure WIFI at their home.

5.3. Source of Smartphone Security Advice

During the interview, we asked the participants about the sources from which they receive security advice and who in their opinion is responsible for raising security awareness among the public. We used an inductive approach on the resulting qualitative data from participants' responses to the question *"Where or from whom do you receive/learn smartphone security advice?"*. The coding procedures were described in Section 4.4. Below, we elaborate on the main codes found in both populations.

Family/friends' past experiences. Unsurprisingly, the primary source mentioned by participants from Pakistan (53.7%) was people's past experiences, whereas 24.5% of participants from Saudi Arabia. We confirm the findings from previous studies conducted on the U.S. population [17], [33], [34]. Participants hear stories from their family members (e.g., husband, daughter, or son) and friends.

Hearing about bad experiences from family members and friends influenced participants' risk perception to avoid similar incidents. The participants reported the negative experiences (e.g., phishing, scam, or theft) that happened to their families and friends. For example, one participant reported a phishing incident that happened with her husband,*"Yes, my husband experienced phishing. He got an email to login and check account activity using a broken link that looked identical to the banks' page but was not secure. He logged in, and the details got stolen. Money was stolen from the account. But thankfully, the government [bank] tracked the criminal, and the amount was restored in the account."*

Internet and Internet Service Providers (ISPs) 16.7% (SA) and 14.8% (PK) specified information on the Internet as another source of receiving security advice. However, 14.7% of the Saudi participants additionally mentioned ISPs as another source of security measures. The largest ISP in the Middle East is STC which offers the majority of Internet, mobile, landline, and television services. It takes measures for security awareness and regularly sends text messages to their customers and displays information on its website regarding avoiding unofficial apps from app stores, ignoring unsolicited text messages, securing connected devices, or using network encryption.

Social Media. Another source reported by our participants, 9.8% (SA) and 14.8% (PK) was Social Media. This is not surprising since 74.4% of our participants use Social Media apps (e.g., WhatsApp, Instagram, Snapchat) on their smartphones. Participants commented that Social Media should be a main source for raising awareness among societies e.g., through video campaigns.

Government. 19.6% of the Saudi participants also mentioned messages, emails, and websites from the government as their source of smartphone security advice. Also, participants suggested conducting awareness campaigns in schools and universities to teach their kids. One participant commented, *"I think the government should have such campaigns that provide information to the general public about threats they may have regarding the security of phones and how to deal with them."*

6. Discussion

Re-validation of rational decision model

Our results confirm Fagan et al. findings and revalidates the rational decision model on a different set of security advice and population with different needs and cultural context. Similar to Fagan et al. results regarding benefits of (not) following advice, the women in our study who followed advice valued the benefit of acting upon the recommended smartphone measures. Those who do not follow the security advice in SA and PK, perceived high benefit of not following advice such as not using a screen lock and not using secure WIFI. For example, women valued the benefit of using a screen lock to prevent their kids from accessing their smartphones, whereas those who do not use a screen lock valued the cost more than the benefits by not enabling the screen lock on their smartphones to prevent their kids from playing with the screen locks (e.g., fingerprint, PIN) and causing more problems. Informing users about the benefits of following security guidelines is helpful but not enough to change their current behavior as prior work stated that such an approach is likely to fail [20], [25], [26].

Similar to Fagan et al. results regarding the cost of (not) following advice, our participants who did not follow the security advice perceived high costs (time or effort) associated with some security advice measures either in SA or PK compared to those who followed the security advice. For example, participants stated that to fulfill their need for Internet they use free public WIFI because of its ease of access and limited effort required compared to connecting to secure encrypted WIFI.

We found that both participants who follow or not follow security advice in SA and PK realized that no risks are associated with following the security advice measures and valued the benefits of following these measures. Similar to Fagan et al. results regarding risk of (not) following advice, the participants who followed the advice rated the risks higher if they stopped following the security advice. The participants who did not follow the advice thought there was no risk associated with not following the smartphone security measures.

Reasons for (not) following the advice. We used affinity diagramming on the discovered codes to get a higher level view of why women in SA and PK are protecting or not protecting their smartphones. Overall, the reasons for (not) following the four pieces of smartphone security advice were grouped into four categories: 1) those that were security/privacy related 2) those where participants saw the risk but their need outweighed it 3) those where participants didn't see the risk 4) others related to convenience. We summarize these themes (participants' reasons) as follows. 1) Security or privacy related reasons: users tend to follow advice often for reasons related to data protection, access control for kids and strangers, privacy, hacking from unwanted messages, and improved performance that comes with security updates/vulnerability patching. 2) Saw risk but need outweighed it: users rejected advice for reasons related to free Internet, easy access to public WIFI vs secured WIFI. 3) Did not see the risk: users also rejected advice for reasons related to considerations such as do not care, not important, nothing to hide, and (no) low risks. 4) Others related to convenience: users followed or rejected guidance for various reasons of convenience. Sometimes following advice was convenient, such as accessing secure WIFI at home. However, at other times, the advice was seen as time-consuming or difficult to follow such as updating the software.

When comparing the reasons for (not) following our four smartphone security advice with those for Fagan et al.'s four computer security advice, users are following security advice often for security or privacy reasons, and sometimes for other benefits. Users tend to reject the advice, and if they do, the risks are perceived as low, or the advice was seen as too costly to follow. For example, users in both studies performed software updates to gain new features as well as increase security. Those who did not follow, did so because they found that updates cause further problems and are time consuming to update. Users in both studies used authentication (screen lock or 2FA) to protect their information and those who did not follow these advice did so because they found it inconvenient to do so. Thus our results provide specific reasons for smartphone specific advice and confirm that differences in risk, cost, or benefit perceptions lead to different security decisions.

Sources of security advice. Studies on Western populations have shown that people often receive security advice from their family/friends' past experiences [17], [33], [34]. Our study confirms these findings on the Saudi and Pakistani women population as the participants indicated one of main source for smartphone security advice was family/friends' past experiences. Most participants hear stories from their husbands, daughters, sons, and friends. Hearing about bad experiences from family members and friends alters their risk perception to avoid similar incidents. However, unlike the studies in the West, we found that **ISPs** are also amongst the main sources of security information for women in SA. Participants mentioned that ISPs take adequate measures for security awareness and regularly send text messages to their customers and display information on their websites regarding avoiding unofficial apps from app stores, ignoring unsolicited text messages, and securing connected devices, etc. Also, 19.6% of the Saudi participants stated that their government should be responsible for providing them security recommendations through different channels such as their official websites, emails, and text messages.

Recommendations. Our findings can help security and privacy researchers in designing educational approaches (e.g., awareness campaigns) and improving the usability of technologies which fit these populations (e.g., notifications of the software updates). Our results suggest the need to address the divergence in women's perceptions and motivations of following security advice using effective risk communication. This can lead to a behavior change amongst those who do not follow the security advice. For example, the use of educational videos that focus on threat and coping appraisals and contain culturally relevant information [12], [13]. Such videos can be campaigned through the Government or on Social media (e.g., WhatsApp) as a large percentage of women use them regularly. Also, presenting the stories of the negative security incidents can be more effective instead of presenting the security facts [33], [41]. Future studies may look into how local norms/culture impact the adoption of specific security advice.

Limitations. Our study is not without limitations. Therefore, the results may be considered exploratory and utmost care should be exercised while generalizing them for the whole population. The main limitation is that the collected data contained a limited number of participants who do not follow two of the security advice measures: screen lock usage and device software update. There is also a size difference between the two sub-samples (about 50%). One of the reasons behind the small sample size is the lack of crowdsourcing platforms in these countries, which mandated the use of in-person data collection through interviews/surveys. Secondly, we did not collect SocioEconomic Status (SES) attributes of participants, e.g., household income, earners' education/occupation. This could have unintentionally biased our sample towards a specific SES class. Lastly, there are many counter arguments to rational model that we did not investigate, e.g., Kahneman cognitive biases [23], [29], [30]. These cannot necessarily be ruled out.

7. Conclusion

Our results validate the rational decision model with regards to (not) following smartphone security advice by women in conservative societies. We find differences in the perceptions of women in conservative societies regarding the benefits, risks, and costs associated with decisions to adhere to four smartphone security measures. Both women who do and do not follow each advice report that their current decision gets them more benefit than if they changed. Those who follow rate the risks of changing their decision as much higher than the risks reported by those who do not follow. The costs of not following are also seen as higher by most that follow compared to those who do not. When looking into the reasons participants gave for their decisions, we find strong trends highlighting the convenience/security trade-off. We suggest launching educational awareness campaigns through videos tailored for this population. These should include risk scenarios of a real incident that happened in these societies via story narration. Lastly, we find similarities (friends and family) as well as differences (ISPs and Government) between the West and conservative Saudi/Pakistani women population regarding the sources of security advice.

References

[1] National centre for cyber security. http://www.nccs.pk.

[2] National response centre for cyber crime. http://www.nr3c.gov.pk.

[3] A study on the mobile phone gender gap in low and middle-income countries. https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2013/01/GSMA_Women_and_Mobile-A_Global_Opportunity.pdf.

[4] Use of smartphones and social media is common across most emerging economies. https://www.pewresearch.org/internet/2019/03/07/use-of-smartphones-and-social-media-is-common-across-most-emerging-economies/.

[5] Saudi arabia social media statistics 2019. https://www.globalmediainsight.com/blog/saudi-arabia-social-media-statistics/, 2019. Accessed: 2019-12-29.

[6] Saudi arabia's cybersecurity concerns increase as threats evolve. shorturl.at/jnZ58, 2019. Accessed: 2020-1-27.

[7] The saudi federation for cyber security and programming. https://safcsp.org.sa/en.html, 2019. Accessed: 2020-1-27.

[8] General authority for general statistics: the unemployment rate. https://www.stats.gov.sa/en/820, 2020. Accessed: 2020-1-26.

[9] Most conservative countries 2020. https://worldpopulationreview.com/countries/most-conservative-countries/, 2020.

[10] N. Abokhodair, A. Hodges, and S. Vieweg. Photo sharing in the arab gulf: Expressing the collective and autonomous selves. In *ACM CSCW*, pages 696–711, 2017.

[11] Y. Al Alhareth, Y. Al Alhareth, and I. Al Dighrir. Review of women and society in saudi arabia. *American Journal of Educational Research*, 3(2):121–125, 2015.

[12] E. Al Qahtani, M. Shehab, and A. Aljohani. The effectiveness of fear appeals in increasing smartphone locking behavior among saudi arabians. In *SOUPS*, pages 31–46, 2018.

[13] 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 *SOUPS*, pages 49–63, 2017.

[14] E. Albrechtsen and J. Hovden. Improving information security awareness and behaviour through dialogue, participation and collective reflection. an intervention study. *Computers & Security*, 29(4):432–445, 2010.

[15] D. Alghamdi, I. Flechais, and M. Jirotka. Security practices for households bank customers in the kingdom of saudi arabia. In *SOUPS*, pages 297–308, 2015.

[16] T. O. Alruwaili. Self-identity and community through social media: the experience of saudi female international college students in the united states. 2017.

[17] S. Das, T. H.-J. Kim, L. A. Dabbish, and J. I. Hong. The effect of social influence on security sensitivity. In *SOUPS*, 2014.

[18] S. Egelman, S. Jain, R. S. Portnoff, K. Liao, S. Consolvo, and D. Wagner. Are you ready to lock? In *ACM CCS*, 2014.

[19] C. Empey. 9 tips everyone forgets to follow on their smartphone. 2019. https://blog.avast.com/9-smartphone-tips-privacy-security.

[20] M. Fagan and M. M. H. Khan. Why do they do what they do?: A study of what motivates users to (not) follow computer security advice. In *SOUPS*, pages 59–75, 2016.

[21] C. Fennell and R. Wash. Do stories help people adopt two-factor authentication? *Studies*, 1(2):3, 2019.

[22] D. R. Foundation. Measuring pakistani women's experiences of online violence. https://digitalrightsfoundation.pk/wp-content/uploads/2017/05/Hamara-Internet-Online-Harassment-Report.pdf, May 2017.

[23] T. Gilovich, D. Griffin, and D. Kahneman. *Heuristics and biases: The psychology of intuitive judgment*. Cambridge university press, 2002.

[24] M. Harbach, E. Von Zezschwitz, A. Fichtner, A. De Luca, and M. Smith. It's a hard lock life: A field study of smartphone (un)locking behavior & risk perception. In *SOUPS*, 2014.

[25] C. Herley. So long, and no thanks for the externalities: the rational rejection of security advice by users. In *NSPW*, 2009.

[26] C. Herley. More is not the answer. *IEEE S&P*, 12(1):14–19, 2013.

[27] I. Ion, R. Reeder, and S. Consolvo. "... no one can hack my mind": Comparing expert and non-expert security practices. In *SOUPS*, pages 327–346, 2015.

[28] R. Jahangir. Women in pakistan most vulnerable to harassment on facebook, whatsapp: report. https://www.dawn.com/news/1455173/women-in-pakistan-most-vulnerable-to-harassment-on-facebook-whatsapp-report, 2019.

[29] D. Kahneman, S. P. Slovic, P. Slovic, and A. Tversky. *Judgment under uncertainty: Heuristics and biases*. Cambridge university press, 1982.

[30] D. Kahneman and A. Tversky. On the reality of cognitive illusions. 1996.

[31] 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.

[32] M. Namara, D. Wilkinson, K. Caine, and B. P. Knijnenburg. Emotional and practical considerations towards the adoption and abandonment of vpns as a privacy-enhancing technology. *PETS*, (1):83–102, 2020.

[33] E. Rader, R. Wash, and B. Brooks. Stories as informal lessons about security. SOUPS, New York, NY, USA, 2012. ACM.

[34] E. M. Redmiles, A. R. Malone, and M. L. Mazurek. I think they're trying to tell me something: Advice sources and selection for digital security. In *IEEE S&P*, pages 272–288, 2016.

[35] N. Sambasivan, G. Checkley, A. Batool, N. Ahmed, D. Nemer, L. S. Gaytán-Lugo, T. Matthews, S. Consolvo, and E. Churchill. Privacy is not for me, it's for those rich women: Performative privacy practices on mobile phones by women in south asia. In *SOUPS*, pages 127–142, Baltimore, MD, Aug. 2018.

[36] C. G. Silveri, H. Bourdeloie, and S. Houmair. Saudi women and socio-digital technologies: Reconfiguring identities. 2017.

[37] Symantec. 5 top mobile security tips to keep your smartphone safe. 2019. https://medium.com/threat-intel/smartphone-security-tips-f0c30c309030.

[38] A. A. Taga. Gender gap in pakistan: A sociological analysis. *Academic Research International*, 2(3):629, 2012.

[39] K. E. Vaniea, E. Rader, and R. Wash. Betrayed by updates: how negative experiences affect future security. In *CHI*, 2014.

[40] R. Wash. Folk models of home computer security. In *SOUPS*, pages 1–16, 2010.

[41] R. Wash and M. M. Cooper. Who provides phishing training? facts, stories, and people like me. In *CHI*, pages 1–12, 2018.

[42] Y. Zou, K. Roundy, A. Tamersoy, S. Shintre, J. Roturier, and F. Schaub. Examining the adoption and abandonment of security, privacy, and identity theft protection practices. In *CHI*, 2020.