CULTURAL FACTORS IN PASSWORD SHARING: A CASE STUDY OF BANGLADESH

by
Aniqa Binte Alam

A thesis submitted to
the Faculty of Graduate and Postdoctoral Affairs
in partial fulfillment of
the requirements for the degree of

MASTER OF COMPUTER SCIENCE

Human Computer Interaction

at

CARLETON UNIVERSITY

Ottawa, Ontario
September, 2021

Abstract

This thesis explores how cultural factors impact password-sharing attitudes of Bangladeshi people. We first proposed "Emics-Etics for Usable Security" framework to incorporate cultural factors in security design. We then conducted a literature review that laid a foundation for applying an Emics approach (culturally specific) to address password-sharing in Bangladesh. To understand password-sharing in Bangladesh, we followed the Emics approach and Grounded Theory method to conduct and analyze interviews of 25 Bangladeshi participants. We found four cultural forces (gender, religion, social norms, and political context) that impact password sharing. We then present our interview-data based password-sharing model that identifies connections between perceived identity and stages of password-sharing, and describe the tensions that arise.

Acknowledgements

First and foremost, I would like to pledge my gratitude to my phenomenal supervisor, Dr. Elizabeth Stobert, for being my guide, advisor, and guardian angel. You have not only helped me to express my ideas in my second language, but also to settle down in my second home country during a global pandemic. Thank you for your patience, encouragement, and kind words throughout my master's journey. I would also like to thank Dr. Robert Biddle, not only for chairing my thesis defense, but also for the countless insightful discussions regarding my thesis and related works.

I would like to thank my thesis committee members, Dr. Hala Assal and Dr. Anil Somayaji. Thank you for your feedback and suggestions, which helped me to make my thesis stronger. A special thanks to baby Paul, for being there and supporting me silently the entire time (Thank you, Elizabeth!). Thank you, not-baby Sylvia and Dr. David Barrera for being parts of this journey. I want to thank my colleagues and friends in the SPIRL lab, especially to Lin Kyi, for her advice and companionship.

I especially want to thank my parents and brother for being the pillars of my strength. I am forever grateful to my husband, Zilani, for loving me, tolerating me during my time of frustrations, and inspiring me to work harder. Thank you so much!

Table of Contents

List of Tables

List of Figures

Chapter 1

Introduction

Developing technical security solutions does not solve the entire security problem; security tools also need to be designed to accommodate human behaviour [23] to be secure. Unfortunately, human behaviour and security often contrast each other: typically, the more secure the system is, the less human factors are accommodated. Password authentication is one such problematic security tool that poses numerous usability flaws. One of the least addressed flaws of the password system is that it is designed to be inherently private and kept confidential, but we notice frequent password sharing in the real world. Moreover, in some cultures, passwords are shared for meeting cultural norms and expectations. Password sharing behavior poses a great threat to software security and privacy for not meeting security policy expectations. When considering how to understand this situation, the questions that came to our minds were: why do people still share passwords when they usually know password sharing is wrong? How does password sharing relate to cultural norms and expectations? Throughout this thesis, the term "we" means I, Aniqa Binte Alam, in consultation with my thesis advisors.

To explore these questions, we at first conducted a literature survey on culture and password sharing. We found literature that distinguished cultures based on the factors like geographical positions, social norms, and people's behaviors: Eastern/Western countries, Hofstede's cultural dimension model [29], and strategic essentialism. However, we found that such cultural differences were generally neglected in usable security research seeming to assume that security is culturally universal.

Password-sharing has been investigated in different countries, for instance, the USA, Australia, Kingdom of Saudi Arabia (KSA), etc., but culture itself was little considered in the methodology of these studies [5,41,67]. When we analyzed available literature on password sharing and device sharing in terms of Eastern and Western

cultures, we noticed that "gender roles" and "respect for parents" played an important role in Eastern countries. In contrast, people from the West usually shared passwords for convenience and necessity.

Motivated by the impact of cultural factors in usable security, we proposed a framework named "Emics-Etics for Usable Security" in our preliminary work. This framework is designed for incorporating cultural differences in security analysis. The Emics (within the culture) and Etics (outside of culture) concepts are two *standpoints* from which human observers can describe a culture [42]. We argue that the security researchers (predominantly westerners) typically follow the *Etics* approach or outsiders' views to understand Eastern cultures, which have often misunderstood and misrepresented version of Eastern values due to a lack of frame of reference. Therefore, the cultural aspects and expectations usually remain unacknowledged. We suggest that security researchers should apply an *Emics* approach or insider's views while designing and evaluating security systems to make the analysis culturally appropriate. We explored our framework using available literature on different security issues.

We wanted to apply our Emics-Etics framework empirically to understand cultural impacts on the uptake and usage of security systems. We chose Bangladesh – an Eastern culture – because I am Bangladeshi; therefore, qualified to conduct the study and analyze the data from an Emics perspective. We chose password-sharing because it has never been explored in the context of Bangladesh in previous literature. We interviewed 25 participants from Bangladesh about their password-sharing experiences in their day-to-day lives. To follow Emics guidelines, we conducted the interviews in Bangla (the native language of Bangladesh), and the interviewer was also Bangladeshi. Using the result of the interviews, we propose a theory to explain password-sharing in Bangladesh.

1.1 Contributions

We offer the following contributions to the study:

1. In our preliminary work, we propose an "Emics-Etics Framework for Usable Security" to understand cultural differences from the viewers' perspectives: that of viewers who live in a culture (*Emics*) and that of those who live outside the

culture (*Etics*). In the main study, we only applied the Emics approach to understanding password sharing in Bangladesh. Etics understanding is out of scope for this study.

2. We provide empirical evidence through a qualitative analysis of the interview data of 25 Bangladeshi participants about what type of passwords, when, why, how, how long, and with what method people from Bangladesh usually share their passwords. Our analysis also found that cultural factors like gender role, social norm, religion, and political context also significantly impact password sharing.

3. Using Grounded Theory, we present an empirically based password-sharing model describing the relationships between cultural factors and the different stages of password sharing experience in Bangladesh. This model will help to incorporate cultural factors in password system design.

1.2 Related Publications and Presentations

A section of this work has been published as a full-paper publication [4] and a poster presentation.

- Aniqa Alam, Robert Biddle, and Elizabeth Stobert. Emics and Etics of Usable Security: Culturally-Specific or Culturally-Universal? In International Conference on Human-Computer Interaction, pp. 22-40. Springer, Cham, 2021.

- Aniqa Alam, Robert Biddle, and Elizabeth Stobert. Emics and Etics of Usable Security: Culturally-Specific or Culturally-Universal? SERENE-RISC Annual Cybersecurity Conference, 2020. **(Best Academic Poster Award)**

1.3 Thesis Outline

The outline of our thesis is given below:

- Chapter 2 lays a background for understanding usable security, culture and password sharing, and Bangladeshi culture based on previous literature. We also explain our proposed "Emics-Etics Framework for Usable Security".

- In Chapter 3, we describe our methodology, reporting study procedures, recruitment, demographic of the participants, and data analysis processes.
- Chapter 4 explains our open codes where we present our data exploring password sharing in terms of who, what, why, how, how long, how it felt, and sharing techniques. This section gives an overview of password sharing in Bangladesh.
- Chapter 5 covers the axial coding phase of our analysis, supported by quotes from the participants. We explain two axes: stages of password sharing and cultural factors affecting password sharing. We also identify our password-sharing model, which emerged from the Grounded Theory process.
- In Chapter 6, we explain the tensions that people face due to the conflicts between motivation and expectations of password sharing. We discuss how these tensions affect relationships and led to interpersonal difficulties, privacy issues, usability issues, and security issues.
- We present our conclusions in Chapter 7. This section discusses our contributions, limitations of our work and suggestions for future work.

Chapter 2

Background

This chapter presents relevant existing literature relating to usable security, culture, password sharing, and Bangladeshi culture. We then elaborate on our proposed "Emics-Etics" framework for usable security, which we applied in our investigation method. A significant portion of this chapter is taken from our HCII 2021 paper [4].

2.1 Usable Security and Culture

The security community has generally accepted the importance of human factors in security, acknowledging security needs to be usable to be secure [61]. Shneiderman characterizes usability through some specific goals: learnability, efficiency, errors, memorability, and subjective satisfaction, which can be achieved by users using the system in a specific context [65]. However, there is no single metric for determining the usability of a system [23].

Usable security researchers usually work on providing tactical security responses to provide immediate results [23]. For instance, one of the earliest works entitled "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0" found that none of the test subjects could complete the given task, which required them to understand and use commercially available encryption software [79]. Another study conducted roughly at the same time, "Users are Not the Enemy" emphasizes trying to understand users rather than the problems [1]. It argues that users are not to be blamed for compromising security; instead, they can become the defence when the rationale for the security measures is explained to them [1]. As in both of these two papers, it is typically accepted in usable security research to consider security systems as culturally universal. Security systems and their ecosystems of use are usually Europe or North America centered and developed by asserting the norms and practices of imagined (Western) users [36]. The usability of security systems is frequently only

tested with Western users or users living in the West. By doing so, the presumption is that "Johnny" [79] from the USA would behave the same way with the system as "Johnny" from Bangladesh. However, previous studies and theories emphasize the consequences of cultural differences in the uptake and use of technologies, including security software [8, 20, 31].

Singh et al. [67] evaluated usability of security in reference to activity, and emphasized trust and user control. The activities that users need to perform have to be easy [67]; however, the utmost security needs to be ensured as well. People perceive security in the simplicity of the transaction process and the availability of support when they make a transaction [67]. The authors think that trust is more important than security. Therefore, a system must preserve human values to gain users' trust and convince them to use it for running day-to-day activities. However, the human values of trust that encourage sharing information among colleagues sometimes make it difficult to comply with an organizational security policy that says not to share information [67]. Besides, the system should also allow users to feel that they are in control of their information. Singh et. al. also discuss the symbiotic relationship between security and privacy and the importance of privacy to ensure security, hinting that system security can be increased by addressing privacy issues related to the system. The importance of privacy is crucial in the banking sector as privacy leaks would cost money and affect personal reputations [67].

Generally, privacy and security are considered as technical phenomena evaluated through the practices of risk, danger, secrecy, trust, morality, and identity [19]. However, Dourish and Anderson argue to consider privacy and security from a holistic view of context as a collective information practice [19]. They propose considering the technical mechanisms (e.g., access control) and related information practices as a collective rather than an individual phenomenon. They also propose analyzing privacy in terms of risk, danger, and morality in social and cultural encounters. Dourish and Anderson also affirm the importance of flows of information in social settings that provides ways to negotiate, demonstrate, and sustain patterns of identity, membership, and affiliation [19]. Secrecy and trust play an essential role in it. Secrets create the social grouping 'us' and 'them' depending on who is eligible to know the

secret [19]. A culture of secrecy and trust make information and its flow meaningful to the people who are involved. In the case of information systems, as the researchers state, "appropriate system design, recognize the information practice, selective sharing of information and its appropriate management, including forgetting and not noticing" are embedded in social groups, and these features create distinctiveness to be identified [19]. Dourish and Anderson advocate for considering collective information practice in security design to contribute to the development of an analytical perspective to investigate security and privacy issues within the borders of social and cultural factors [19].

2.2 Culture

To incorporate cultural factors in security systems, we first need to understand what culture is. Although culture does not have any specific widely accepted definition, one of the most common approaches defines it as "patterns, explicit and implicit, of and for behavior acquired and transmitted by symbols, constituting the distinctive achievements of human groups ... [and] ideas and their attached values." [43].

In other words, culture refers to what a group or society believes to be true that forms some common values and norms [6]. People's perceived values and norms define what they will consider good or bad and acceptable or unacceptable, which creates a set of rules about behaving and performing tasks [6]. Cultures can be of different levels and sizes; for instance, "Western culture," "US culture," "gang culture," and even "family culture" [6].

In our literature survey, we categorized literature based on how the participants of the studies (or countries of focus) have experienced the consequences of digital colonialism [44] – the East (digitally colonized) and the West (digital colonizers). The West refers to the countries that possess (or have historically possessed) dominating technological power and current sources of geopolitical and cultural epistemic inequalities. The Eastern countries experience the consequences of these epistemic inequalities. Our work uses the terms "East" and "West" beyond their geographic meaning and cultural differences to symbolize cultural and intra-country inequalities. The terms are relative to each other, meaning one country is considered as West in

respect to the countries it dominates or vice-versa. For instance, the USA, Canada, and the UK would be considered to have colonizing power in respect to countries like Bangladesh, India, and Pakistan, although historically, Canada and the US were also colonized by the British (as well as French and Spanish).

Strategic essentialism [69] refers to how minority or ethnic groups create a temporary/long term sense of collective identity setting aside their cultural differences [18]. For instance, many cultural, religious, and linguistic groups in India come together as "Indian" in terms of their common colonization by the British [18]. This notion is essential for collective political movements and feminist studies. However, for our work, we argue for the impossibility of essentialism in the context of security design and acknowledge intra-country cultural differences. For instance, by our definition, Australian aboriginal groups are considered as East (digitally colonized), although Australia as a country is considered as the West (digital colonizer).

Hofstede's Cultural dimensions model [29] is the most well-known framework for cultural differences. He proposed four (later six [30]) cultural dimensions to distinguish the differences among national cultures: power distance, uncertainty avoidance, individualism-collectivism, and masculinity-femininity. Power distance refers to the extent to which the less powerful group accepts the power inequalities [30]. Power distance scores tend to be higher for Latin, Asian and African countries and lower for Western countries [30]. Uncertainty Avoidance (UAI) refers to society's tolerance toward uncertain situations [30]. For instance, Bangladesh has higher UAI score (60) compared to the UK (35), meaning people from UK are more comfortable with uncertain situations [32]. In individualistic cultures, people usually feel they should take care of themselves. In collectivistic cultures, the groups take care of their members. Individualism scores tend to be higher in Western countries, and collectivism scores tend to be higher in Eastern countries [30]. Lastly, masculinity refers to a preference for materialistic choices, whereas femininity refers to a preference for caring and quality of life [66]. The masculinity score is higher in Western countries. Hofstede's model has been widely criticized mainly because it assumed all national people as a homogeneous entity; however, this model is still considered useful in organizations [37].

If we incorporate East-West segregation with Hofstede's model, it can be conjectured that Eastern cultures are collectivistic and feminine and would have a higher score in power distance and uncertainty avoidance. In contrast, Western cultures are individualistic and masculine with a lower score in power distance and uncertainty avoidance. For example, Bangladesh (an Eastern country) has higher power distance (80) and uncertainty avoidance (60), and lower individualism (20) and masculinity (46) scores compared with the USA (a Western country) which has higher individualism (91) and masculinity (62), and lower power distance (40) and uncertainty avoidance (46) scores [32]. This demonstrates that some Eastern countries have low uncertainty avoidance score and some Western counties have high uncertainty avoidance score, which indicates that there is greater complexity in understanding East and West than is shown in Hofstede's model.

2.3 Password Sharing

Almost everyone in the industrialized world needs to interact with passwords multiple times daily, but passwords are a problematic system with numerous flaws. One of the least addressed issues with password systems is that they do not provide safe password sharing. Passwords are designed to be inherently private and secret, disregarding the fact that in some cultures, social norms and family values *require* them to be shared. As a result, people frequently share their passwords for banking, social media, and entertainment accounts [5, 41] following insecure procedures: writing them down on paper or sending them through SMS, email, and social media.

The usage dimensions of mobile phones have expanded these days: people can now use them as their mini computers [40]. They can generate and store contents e.g., photos, audio files, video files, and messages) on mobile phones and share them with social contacts using different applications. However, the security model of the mobile phones is still binary (locked/unlocked) as they are primarily designed to be private devices following the "one account, one user" privacy model [40, 60]. In practice, mobile devices are shared for various reasons by either sharing the phone PIN or by opening the phone lock, which challenges this definition and architecture [2,40,56,60], and weakens security.

2.3.1 Security Implications of Password Sharing

Password sharing can cause harm to both business owners and individuals. When a malicious user obtains passwords due to password sharing, it can result in credential fraud, account compromise, monetary loss, and cyberbullying [48]. According to Parks Associates, the pay-TV industry was projected to lose USD 6.6 billion in revenue from password sharing and movie piracy in 2019, and the number could grow to USD 9 billion by 2024 [24]. In 2010, the Kingdom of Saudi Arabia suffered the seventh-highest incidence of security breaches, although they had only 0.007% of internet users in the world [5]. One of the identified causes is password sharing behavior among co-workers and family members [5].

Password sharing also has negative security and privacy implications in personal life. For example, one of the respondents in a password-sharing study had a distressing experience sharing passwords with her boyfriend. He sent threatening emails from her email account after their breakup to destroy her reputation [41]. Similarly, mobile phone PIN sharing can also cause both privacy and security issues. In 2012, around 12% of US mobile phone owners reported experiencing unauthorized access that they perceived as a violation of their privacy [9]. One of the most common privacy invasion scenarios is when parents, siblings, friends, relatives, and strangers ask to use the owner's phone (most of the time, they ask to share PIN or open the lock in front of them without trying to hide the password input) for a specific task (e.g., taking a photo, playing a game, or making an emergency call) and then browse through the personal data [3, 17]. Mobile device sharing may lead to leaks of private information, as well as changes to data, both intentional (e.g., writing a text message as an impostor) or unintentional (e.g., deleting contents or changing app settings) [27]. These also bear emotional consequences for both owners and attackers. The positive and negative sentiments resulting from unauthorized access incidents include amusement, satisfaction, relief, annoyance, anger, guilt, humiliation, pain, regret, sadness, and shame [17]. Sometimes relationships are ended as a consequence of negative emotions. Obada-Obieh et. al. [52] studied the challenges of *ending* password sharing and found that people both experienced cognitive and psychological burdens when ending password-sharing. People need to remember with whom the passwords are

shared and where they have reused them. Changing passwords for ending sharing also require them changing the reused passwords. Despite having bad consequences and experiencing burdens of password sharing, people still share passwords for various reasons.

2.3.2 What Passwords are Shared and with Whom

Previous studies explored what type of accounts were shared and with whom they were shared. Kaye [41] designed a survey to understand what type of accounts: for instance, email, work email, Facebook, instant messaging, Amazon, eBay, smartphones, and computer passwords, etc. He also found that people shared their passwords with partners/spouses, parents, sons, daughters, colleagues, and friends. People from the United States, India, New Zealand, Canada, the United Kingdom, and Australia participated in the survey. He found that one-third of the total respondent shared their email credentials, a quarter shared their Facebook credentials, and one-fifth shared their work passwords. The study found women shared slightly more passwords than men. Men aged between 46-49 shared more passwords than the age groups 13-39. People frequently shared passwords of their office workstation and library access with colleagues and friends. In family settings, other than sharing Wi-Fi passwords or the passwords of subscribed sites (e.g., Netflix, Expedia, etc.), people were often found to share email credentials with family to check emails in case of emergency (like traveling). Previous studies also found that people also shared their banking credentials with parents, spouses, and sometimes with non-relative relations in different cultural contexts [5, 67]. People also frequently share their mobile devices and PINs for various reasons [2, 40, 56, 60].

Password Sharing among Couples for Trust and Convenience

Previous research found password sharing among couples was prevalent in different cultures. Singh et al. ran an interview-based qualitative study between 2005-2006 to understand the practice of sharing banking passwords of Australian users [67]. Even in the context of a strict banking policy that prohibits sharing online banking passwords and PINs among friends and family [67], the study found that couples

(both married and de facto) share their online and mobile banking passwords with each other. The finding of the study states that the couples share online and mobile banking passwords because of trust, convenience, and the distribution of household work. Some of the participants have private individual accounts, but the partners knew the reasons for them being private (e.g., having mother/children from other marriage to take care) [67]. It was also found that couples chose only one person in the relationship to handle the accounts [67].

A similar study was published in 2015 in the context of the Kingdom of Saudi Arabia (KSA), and it was found that couples (only married) shared their passwords because it was considered as a 'need to know' factor for them rooted in mutual trust and convenience [5]. In KSA, men often manage both partners' accounts since women usually do not have physical access everywhere. In almost all households, wives are financially dependent on husbands. Therefore, husbands usually inform their wives of their banking credentials and asset information in case of an emergency. Both men and women consider mutual trust and convenience are the reasons for sharing passwords with partners. Women usually think that their partners are entitled to know their credentials [5].

Couples from both Eastern and Western cultures share mobile devices, but gender plays an essential role in sharing. In Eastern cultures, both of the partners check each other's phones, but the wife typically does so in secret. The husband does it openly because of culturally accepted gender superiority [60]. Sometimes women rely on their husbands for technical help with mobile devices. For example, wives take help from their husbands to log in to their social media accounts [60]. Sometimes, monitoring is viewed as coercive. For example, some women from Bangladesh reported that their husbands installed spyware for tracking their usage [60]. They reported feeling upset and described their coping strategy, which is to call their parents using colleagues' and friends' mobile devices [60]. In the West, couples share their devices because of proximity and convenience. For instance, while watching TV, one person may use their partner's mobile device to play games just because it was nearer [47]. Partners also answer calls or access devices to help navigate when the other person is driving [47].

Sharing Password as a Means of Necessity

Previous studies indicate that colonial banking authentication systems and legislation do not acknowledge cultural practices like money and property sharing among extended family members. In turn, this hampers the banking accessibility of different disadvantaged groups of different cultures. For instance, Singh et al. found in their work that people from rural and remote Aboriginal and Torres Strait Islander communities in Australia usually share bank cards and PINs with both family members and clan members [58, 63, 68]. Some members of the Ngukurr Aboriginal people of the Northern Territory in Australia share their banking cards and PINs with their school-going children so that they do not get "shamed" in front of the non-Aboriginal community for not having enough money [63]. Another common practice in Australian Aboriginal communities is "book-up": a system to take a small and short term loan from stores, taxis, hawkers, and airlines by sharing debit cards along with PIN as a security check [68]. The book-up process carries clear risks, but without this process, short-term credit would be otherwise unavailable [59]. The banking authentication system also does not give any solution for areas where physical banking is inaccessible. For instance, in the Torres Strait Island communities, there are 17 inhabited islands but only one island (Thursday Island) with a bank [67]. To access the banking facilities from other islands, people usually have to book tickets, prepare to stay overnight, and spend around AUD 250-300 depending on the season. Hence, as a matter of survival, when one person from a remote island goes to Thursday Island, they do everyone's shopping and other business by taking their bank cards and PINs [67]. In New Zealand, Maori people may share ownership of the land and houses; but, banking systems do not allow them to access loans with shared property [39].

Mobile devices are shared with family, friends, and neighbors in rural and underdeveloped areas because of a lack of affordability. In rural parts of Kenya, only wealthy families can usually afford a mobile device [50]. In these households, the device owner (usually the male head of the family) becomes the tech-savvy user and performs tasks on behalf of others [60]. This situation also gives rise to small businesses: people who cannot afford a mobile device can pay to use another's device to communicate [21]. Similarly, in some parts of rural Uganda, mobile money is used to

pay for goods and services [78].

Password sharing is also sometimes essential for people with disabilities. This special group mostly prefers telephone and internet banking depending on their disability [67]. They need to share passwords both in terms of physical interaction with bank staffs or to use the ATM machine. It was found that the majority of the people with disabilities needed to share their access code to buy goods from the mall [67].

Password Sharing with Parents

Family values in some cultures situate parents in esteemed positions. As a result, it is culturally expected that parents should know their children's (even adult) monetary status, including banking passwords. For instance, both men and women in KSA believe that fathers should know the banking passwords of their children as they have 'rights' over their children's money [5]. Women in KSA share their passwords because their fathers monitor and safeguard their finances even after their marriages, whereas men give banking access to their fathers out of respect. If men wish to revoke such access, they are perceived as 'mature' in the family rather than secretive. Women would share the credentials with mothers to safeguard their money as well. For men, the majority of them would prefer to share credentials with mothers rather than their wives. If the father dies in a family, the eldest son gets his position and handles the accounts of the younger family members as the father would do. There has been little work on password sharing in other Eastern cultures; however, we assume, family values and parent-children relationships in many Eastern countries may follow a similar pattern to the KSA.

Device sharing is also common in parent-children relationships. In some Eastern countries, family members often charge their phones in the same place, and children can access their parents' accounts anytime, even after owning mobile phones by themselves [70]. The father figure usually bears the mobile phone cost of everyone in the family [70]; hence, it is perceived as normal if the children make phone calls from their parent's phones or vice-versa. A study of Pakistani users found that women's (mother figures) devices are usually considered by default as a "family device" [60].

Some women from Bangladesh reported that their children used their phones for playing games and watching videos; however, children usually did not touch their father's phone. Parents usually have unlimited access to their adult children's devices in some cultures. If parents want to check their children's mobile devices, children usually comply with upholding the image of being "good", however, parents sometimes secretly spy on their children's usage [60].

Family values are often different in Western cultures. For instance, although parents usually know the passwords of their children when they are young, it becomes a case of family negotiation when they become teenagers [41]. Both Eastern and Western children may know the passwords of their parents or grandparents only if the parents or grandparents cannot set or remember their passwords themselves [5,41]. In Western cultures, minor children who do not own mobile devices usually get access to their parents' mobile phones. Adult children get access to their parents' devices only in case of necessity or accident. For instance, if the parents are not technologically adept, adult children often offer technical support and manage accounts for their parents [47]. Parents sometimes monitor their minor children's browsing histories when they share the same devices. However, parents usually do not tell their children about this [47].

2.3.3 Previously Proposed Solutions to Password-Sharing

Security researchers usually consider password-sharing as a bad habit, and a harmful behaviour for security and provide technological and policy-based solutions to mitigate this behaviour. Frequent password resets and the use of biometric passwords are some common suggestions to limit this behaviour [24]. For instance, Mandujano and Soto propose a system for tracking keystrokes to limit access if the keystroke dynamics are changed when used by different users [46]. One commonly cited advantage of graphical authentication systems is that they are more challenging to describe and share because they are not simple text strings [7]. Password policies can also be designed to decrease password sharing [64].

Some researchers investigated the importance and necessity of password sharing and proposed solutions indicating secure password-sharing. For instance, Singh et.

al. propose that the design should consider the context, physical status, social relationships, social and cultural values and norms related to password sharing [67]. The authors believe that accepting password sharing is inevitable for the conveniences it provides. Incorporating it in the design would ensure higher usability and security for the people from different cultures.

One approach to addressing mobile device privacy is to enable multiple user accounts. Multiple user access was introduced in Android version 4.2 (API 17) in November 2012, and restricted profiles were introduced in version 4.3 (API 18) in July 2013 [57]. Using multiple user accounts, the device owner can create, delete, and modify secondary accounts [25]. Secondary accounts are password-protected, and the secondary account holder cannot view the device owner's data, nor make changes in the device (e.g., update and download apps) but can use the owner-selected apps [57]. However, this mechanism has not been found to be usable in different Eastern cultures. It should also be noted that this feature has never been introduced on devices running iOS, further restricting the usefulness of this alternative for many users.

Sambasivan et al. suggested some improvements for the mobile device sharing issue, including improved discovery of privacy controls, content hiding features and algorithmic understanding of multiple user use cases [60]. The authors also emphasized using the culturally appropriate text while designing technology systems so that Eastern users do not perceive them as a Western concept.

2.4 Bangladeshi Culture

By the World Bank's estimation, Bangladesh is a "lower-middle income" country in South Asia with a GDP growth rate of around 8% a year [49, 74, 77]. It is the eighth-most populous country globally, having 170 million people [74]. The majority of Bangladeshis identify themselves as Bengalis (98%), and the rest 2% as ethnic minority groups [62].

Historically, this region struggled with colonialism, the partition of India in 1947, and the 1971 Bangladesh Liberation War [62]. After 50 years of independence, Bangladesh has not only showed fast-paced economic growth, but child education rates (e.g., 98% of Bangladeshi children finish primary school), and vaccination rates

against diseases like polio (immunization rate risen to 80%) have also increased rapidly [73, 74].

2.4.1 Religion

Bangladesh is officially a secular nation but Islam is mentioned as the official religion in the constitution. Bangladesh has the fifth largest Muslim population globally, with 89.1% of its population following Islam [75]. Hindus constitute 10% of the population and the rest 0.9% of the population follow other religions, including Buddhism and Christianity [62].

The relationship between Islam and Bangladesh is complex. The partition of India in 1947 and the unification of Punjab and other areas in the west (current Pakistan) and East Bengal (current Bangladesh) to become one Pakistan, reinforced the reality of Muslim-Bengali formulation [13, 33]. On the other hand, several movements in the late 1960s and the 1971 Liberation War of Bangladesh took place in the form of a "Bengali ethnic and language-based struggle" against economic, cultural, and political exploitation by West Pakistan (current Pakistan), downplaying the Muslim identity of about 90% of the country's populations [33]. Historically, it is apparent that Bangladesh's Muslims have switched from 'Bengaliness' to 'Muslimness' as the situation demanded [15]. In current Bangladesh, Bengali ethnicity remains a marker of identity along with a slightly suppressed Muslim identity. As a result, Bangladesh is now recognized as a "moderate Muslim nation" by the Western world [33].

It is vital to understand the dual identity of Bangladesh's major population—- "Bengali–Muslim" or "Muslim–Bengali"— to comprehend Bangladeshi culture. This dual identity of Bangladeshi people plays a significant role in personal, social, cultural political lives.

2.4.2 Family

Family is the center of social life in Bangladesh. A family usually consists of husband and wife, their unmarried children, their adult sons, their wives, and children [62]. They all live in the same household. Sometimes the paternal grandparents also live in the same household. Bangladeshi people also maintain close relationships with

relatives. The father of the family is the decision-maker for essential issues like finance. The eldest woman (mother or grandmother) usually decides on domestic issues like groceries. Generally, children are expected to consult their parents on major life decisions like education, career, and marriage [62]. Dating is not socially accepted in Bangladeshi culture, and it is usually conducted secretly without the consent of the parents and elder relatives [72]. Many marriages are still arranged, and parents usually decide when their children will get married and to whom. Even if children choose whom to marry, they usually do not marry without their parents' permission.

2.4.3 Patriarchy, Islam, and Harassment Against Women in Bangladesh

Bangladesh is a patriarchal society meaning men hold power and control of resources, and women are usually in charge of household work but financially dependent on men [14,22]. Religion plays a significant role in defining such patriarchal elements. For instance, a misinterpreted version of Islamic rule is typically believed in Bangladesh that men's job is to earn for the family and women's job is to serve their husband and manage the household [14]. Sometimes, men dominate and oppress women through patriarchy; however, the situation of women has improved recently: women's participation in the paid workforce rose to 36% in 2019 [74]. Women are still vulnerable in society, and violence against women usually goes unchecked due to lack of legal consequences and social stigma [73].

Women in Bangladesh fear sexual harassment, which is very common in society. It is easy to harm women in this culture, and women are sexually harassed on the streets, in the marketplaces and in every institution, even online [14, 34]. Cyber harassment of women in Bangladesh has risen significantly. One study confirmed that around 73% of female internet users reported cyber harassment [51]. Hacking, fake IDs, harassment and defamation, cyber pornography, financial fraud by mobile, blackmail and extortion, and terrorist activity are common forms of cyber harassment complaints [38]. When women face harassment in Bangladesh, they usually walk away pretending not to notice rather than giving any response [26, 51]. Such passive response is also typical in the case of online harassment. Women are also always insecure without men's company— their fathers, elder brothers, and husbands.

Sometimes, the company of a younger brother is considered a more secure option for women than being alone. These men in women's lives also behave protectively in a similar manner when women use the internet and social media.

2.4.4 Cultural Norms

Bangladesh is a collectivist country. For this, the general approach to family ties is communal. People often act in the best interests of the family and extended family rather than based on their individual preferences [62]. Office colleagues and friends also sometimes become family friends and are treated similarly. Generally, people respect older people and obey their words. Criticizing elders or disregarding their opinions is not accepted. Bangladeshis usually speak indirectly, avoiding strong words, assertions, or confrontations [62]. It is not socially acceptable to say *no* on the face of it to any requests. They either comply with the request to avoid saying no or phrase objection as 'I can try' [62].

2.4.5 Political Context

Bangladesh currently does not have a very amicable or democratic political context. The Economist describes it –"Bangladesh's politics is as depressing as its development is uplifting" [74]. Bangladesh is considered likely to become a one-party state. For instance, before the most recent election in 2018, opposition parties claimed that more than 7000 of their activists had been arrested, and many candidates were barred from running the election, which resulted in a massive win by the Awami League [74]. The current government also could abolish new candidates to coming into politics. For instance, when Nobel peace prize winner and the founder of Grameen bank (the biggest provider of microloans to the poor) Muhammad Yunus wanted to start a political party, he was ejected from Grameen Bank, and he was unable to start any party [73].

Freedom of speech is also in question in Bangladesh. Recently, a writer and cartoonist named Mushtaq Ahmed as arrested after criticizing the government's response to Covid-19 on Facebook, and he died in prison allegedly of torture [74]. Journalists and other critics of the government have also been arrested under the "Digital

Security Act" passed in 2018 [74].

2.5 Emics-Etics Framework for Usable Security: A Culture-centric Framework to Address Usability Problems with Security Tools

There have been different culture-centric frameworks proposed for incorporating a range of methodological possibilities to understand a variety of topics [11]. One of the most widely used frameworks for investigating cross-cultural issues is known as *Emics-Etics* [10,45,55,76]. In our preliminary work, we conducted a literature survey study to apply the concept of Emics-Etics to identify the implications of cultural differences in usable security and we named our framework the "Emics-Etics for Usable Secuity" [4].

Historically, the terms Emics and Etics were derived first in linguistic analysis [55]. The term *Emics* is adapted from phonemics, and refers to the sounds that are specific to a particular language in a particular culture [12]. Phonemic analysis refers to the sounds of any language that change the meaning when they are a part of words [11], e.g., pin vs. bin.

The term *Etics* is adapted from phonetics and refers to sounds that are the same in all languages [12]. Phonetics considers the taxonomy of the body parts that are active in producing sounds (e.g., vocal apparatus) that are used to develop a systematization of meaningful sounds [11,28]. For example, the distinction between initial 'L' and the initial 'R' is absent in the Japanese language; therefore, Japanese speakers usually find it hard to differentiate these sounds when speaking English [11].

The Emics (within culture) and Etics (outside of culture) concepts are also widely used as a cross-cultural framework. They are considered as two *standpoints* from which human observers can describe culturally-specific (Emics) and culturally-universal (Etics) human behaviours [42].

An Emics analytical standpoint is internal and holistic and can distinguish and understand the intrinsic cultural values of a society [42]. On the other hand, an Etics analytical standpoint is external or alien and often misunderstands and misrepresents the *other* cultural values due to a lack of a frame of reference [11]. For example, an Etics perspective on credential sharing would criticize users for sharing their banking

passwords with family members, but an Emics perspective would recognize the gender roles that limit the ability of women in the Kingdom of Saudi Arabia (KSA) to independently visit banks, leading them to share their passwords with trusted male relatives [5].

Our Emics-Etics based cross-cultural framework considers the East-West dichotomy to understand cultural factors in security and privacy applications. Computer security is likely to be designed based on Western values as the majority of the computer infrastructures have been built in the West [29, 71]. Some Eastern countries, for instance, China and India, are getting into the technology development sector; however, they follow mostly existing Western designs in their products.

We argue that security community (typically West) follows the *Etics* approach to understand Eastern values while designing and evaluating security. Since Western designers do not integrate into Eastern culture to understand the cultural values, they often misunderstand and misrepresent Eastern values due to a lack of a frame of reference. As a result, Eastern people sometimes find the security systems alien and hard to understand even though West assumes they are culturally universal. In this paper, we suggest that researchers should apply an *Emics* approach while designing and evaluating security systems to make them culturally appropriate.

Usable security is difficult to achieve and there is always room for improvement in security. One of the impediments to increasing the usability of security systems is the practice of Western ethnocentrism while designing security tools that results in digital domination. Our framework provides an approach to acknowledge culturally specific practices in security design.

2.5.1 Application of Emics-Etics for Usable Security Framework

Our preliminary work is based on an extensive literature survey. In this work, we proposed Emics-Etics framework to explore cultural-centric security issues and analyzed related works about three security challenges for both Eastern and Western cultures: software piracy, password sharing, and mobile device sharing [4]. Using a literature review, we identified flaws in current security solutions that stem from following an Etics approach and provided some solution approaches using Emics. A summary of

our findings from literature survey is presented in Tables 2.1, 2.2, 2.3. Table 2.1 shows issues for password sharing, which led to our main study.

Table 2.1: Summary of approaches to password sharing.

Etics Approach	Emics Approach
• Password sharing is dangerous for security • Technical solutions are required so that people cannot share passwords • Legal frameworks should limit password sharing • Strict password policies limiting password sharing should be applied	• Password sharing is a cultural norm – Family members share passwords with each other because of trust, power role, convenience, and social expectation – Gender norms do not always allow women to access banking and other services • Family expectations, geographical disadvantages and lack of infrastructural facilities create necessities of sharing password

In our work, we find significant cultural differences in security attitude, and we suggest that cultural factors (e.g., trust, family values, and social norms) must be considered while designing and developing security mechanisms. One can argue that Western countries also face the similar problems that we discussed in our study. However, we tried to highlight through our framework that the approach to the similar problems should be different based on the cultural context. In our work, we do not mean to imply that universal components do not exist (for example, the memorability problems of passwords appear to be culturally universal), only that we cannot treat all security problems and solutions as universal and independent of culture. We envision a culturally-inclusive security environment where Etics will be ideally applied to identify our universal components and Emics will explore the claimed universality of them and examine cultural factors affecting them.

Table 2.2: Summary of approaches to software piracy.

Etics Approach	Emics Approach
• Legal frameworks in Eastern countries need to be strict • Law enforcement in Eastern countries needs to be strong • Less corrupt governments would strengthen both legal frameworks and law enforcement • People should be taught that piracy is morally wrong • Impact of *globalization* may reduce piracy in the long run	• Concept of *intellectual property rights* is 'foreign' to Eastern people • Software sharing is a socially accepted norm • Software prices should be cheaper in Eastern countries • *Collective morality* does not consider piracy a 'wrong' deed because it does not create any direct harm to anyone • Technology sharing is considered a part of the 'community well-being' as not everyone can afford software/product • Gender and religion have impact on piracy

2.6 Summary

The literature provides strong evidence that the users from Eastern cultures share their passwords despite facing problems. The password systems usually do not acknowledge the cultural and social values of the Eastern users. As a result, they end up engaging in security-compromising activities. However, no study has yet directly investigated cultural factors involved in Eastern people sharing their passwords. The literature also suggests that Bangladesh is a collectivist country having both a strong cultural and religious identity. Password sharing had never been studied in the context of Bangladesh.

Based on our understanding of the importance of culture on security behavior, we proposed our "Emics-Etics" framework, which suggests following an Emics approach

Table 2.3: Summary of approaches to mobile device sharing.

Etics Approach	Emics Approach
• Mobile devices are designed for personal usage only • Unauthorized device sharing violates users' privacy • Technical frameworks are required for secure device sharing. For example, – Android's Multiple Access Mechanism for multiple accounts – Software for hiding private files	• Authorized or unauthorized device sharing among family, friends, colleagues, and community is culturally accepted • People share devices because of trust, necessity and social expectation • Android's Multiple Access framework does not work in East because it is not accepted to "openly" hide information from family • Mobile device sharing with community is required because not everyone can afford a mobile phone

while designing culturally appropriate security tools. We address all of the above-mentioned research gaps in the following sections by applying the Emics approach to investigate the password-sharing attitudes of Bangladeshi people.

Chapter 3

Study Methodology

Our literature survey suggests that the users from Eastern cultures might face usability issues and engage in security-compromising activities because security systems do not acknowledge their cultural and social practices. Based on this understanding, we proposed our "Emics-Etics" framework, which suggests following an Emics approach while designing and evaluating security systems to make them culturally appropriate. Our research questions were:

1. Why do people from Bangladesh share passwords?
2. How does password sharing relate to cultural norms and expectations of Bangladeshi people?

To understand how cultural factors affect the behavior of Bangladeshi users in terms of password sharing, we used our proposed Emics approach. We gathered qualitative data from Bangladeshi users using our framework. We also wanted to create a theory of password sharing solidly based on empirical data. For this reason, we decided to use the Grounded Theory approach. We received ethical clearance for this project from the Carleton University Research Ethics Board B, clearance number 114925.

3.1 Study Overview

To investigate how and why people from Bangladesh share their passwords, we conducted a semi-structured qualitative interview study about their password-sharing attitudes and expectations. We used our "Emics approach" to design our study. We wanted to run our study in an Eastern country to identify the cultural issues related to password sharing. We chose Bangladesh, an Eastern country, because the lead researcher is from Bangladesh and Bangla is her native language. Thus, running the

study by a Bangladeshi researcher supports the fundamental idea of our framework: research should be conducted by and situated in the cultural constraints surrounding it. Our study is designed in three parts: pre-screening survey, interview session, and analysis.

Before inviting the participants to the interviews, we asked participants to fill out a pre-screening survey to show their interest in the study. We designed the pre-screening survey to determine the eligibility of our participants and ensure their diversity. We asked them about their demographics, including gender, age, educational background, physical and digital account usage, and whether they share passwords or not. An audio recording was mandatory for our study, so we asked participants whether they agree to be audio recorded or not. We did not invite participants who did not agree to be audio-recorded. There were 13 questions in the survey. We used Qualtrics to conduct our survey. It took approximately 5 minutes to finish the survey. Participants were not compensated for finishing the survey. The pre-screening survey questionnaire can be found in Appendix B. 188 participants completed the survey.

Eligible participants were invited to participate in our interview session. Due to the COVID-19 pandemic, we conducted the interviews virtually using Zoom. We conducted the interviews ourselves. Some of the questions were based on the survey answers; for example, if someone mentioned that they used smart TV, we asked them directly whether they shared the password of the smart TV and how they shared it. We also asked follow-up questions, asked new questions based on the answers given, and encouraged participants to give elaborated answers. We never asked participants to share passwords with us and we reminded them not to do so several times during the interviews. Due to the time difference between Canada and Bangladesh, the researcher had to take most of the interviews during late night or early morning in Canadian time. Each interview was 45-50 minutes long. All the interviews were audio-recorded. Our interview guidelines can be found in Appendix B.

We asked our participants in the pre-screening survey about their preferred language (English or Bangla) for the interview. Most of our participants chose English, possibly because formal meetings are frequently conducted in English. However, after conducting the first two interviews in English, we realized that people sometimes do

not find words to describe a particular situation and ended up using Bangla to make the researcher understand that. We then decided to conduct the rest of the interviews in Bangla even though the participants chose English. The researcher started the interview in Bangla proactively and told the participants that they could use any language (Bangla or English) to answer. None of the participants chose English afterward but answered using a mixture of both languages.

We noticed that participants felt comfortable sharing their experiences because the interview was conducted by the Bangladeshi researcher. They expressed their comfort by saying things like, "you know how Bangladeshi parents monitor their daughters...we all know it" or "you know how brown mothers are". Although the researcher understood what they tried to mean, she still asked further questions like "what do you mean by this?" just to validate whether her understanding was correct or not.

3.2 Recruitment

Between February and March 2021, we recruited 25 participants for the final interview. The participants were recruited from the lead researcher's connections in Bangladesh. This included distributing the recruitment materials on social media, previous workplace, and university platforms. We prepared recruitment materials in both English and Bangla. We prepared the English recruitment materials first (email, poster, consent from etc.) and then translated them into Bangla. We used a snowballing method by asking people including the interview participants to share the recruitment materials in their network.

The inclusion criteria were being over the age of 18, being comfortable giving an interview in Bangla or English, able to use Zoom, and being a user of technology devices including computer/mobile phones, may use the internet and social media, and may (or may not) have previous password sharing experiences. We also wanted to know why participants did not share passwords. The researcher excluded the participants whom she knew in real life.

Interested participants were asked to fill out a pre-screening survey questionnaire. The researcher then sent out a batch of invitations (5-10) to the selected participants

who met the selection criteria. We wanted to have diverse participants; therefore, each batch maintained gender and age ratios. The participants were asked to digitally sign the consent form in Qualtrics and schedule a Zoom meeting in Calendly. We sent out approximately 80 email invitations and 40 of them consented to participate. 15 of them did not show up and did not respond to any emails of the researchers afterward. We stopped recruiting participants after the interview data had been sufficiently saturated. Participants were compensated BDT 1000 (approximately 15 CAD) for participating in the interview.

3.3 Interview Participants

We interviewed 25 participants for the study. We reached saturation at the 25th participants, where we did not hear any new information. We had 11 female participants and 14 male participants. Participants' age ranged from 18-49, and 60% of our participants were aged between 18 and 29. Among our participants, 9 of them were students studying engineering, science, social science, and humanities. The other participants (15) worked in banks, private companies, marketing agencies, medical centers, and pharmaceutical companies. One of our participants was on a work break. The overview of our participant demographics are given in Table 3.1.

3.4 Analysis

After the interview, we anonymized the interview recordings and deleted any additional data saved during the interviews (for instance, a chat log). We then transcribed and translated them into English for further analysis. We first transcribed and translated the anonymized interviews from audio recordings. We then rechecked our translation before deleting the recordings. While translating from Bangla to English, we realized that it was sometimes hard for us to depict the exact feelings of the participants in English. For instance, one of our participants described his wife as from an "analog period" because she did not want to use a smartphone. When the other researchers read the quote, they thought he was belittling his wife. However, the lead researcher knew that he was not belittling; rather, there was an emotion of

love and complaint when he talked about his wife. This is one of the limitations of our work that we might not always successful in translating the feelings into English. We did not use our survey data for further analysis.

We followed the Grounded Theory methodology [16] for the qualitative analysis. We first analyzed the data "line by line" and incident by incident to assign codes in open coding. In the axial coding step, we looked for relationships in the open codes. Due to COVID-19 lockdown, we could not access our lab; therefore, we ran the analysis using different software and collaboration tools. They were -

NVivo: We used NVivo, a qualitative data analysis software, for the initial coding of our data. We uploaded the interview translations in NVivo and coded them line by line. NVivo gave us the flexibility of coding the labels, editing them, or removing them anytime.

Miro: We also used Miro, an online whiteboard and visual collaboration platform. We created the sticky notes of all our open codes. We then collaborated online to group our codes.

The processes of open coding and axial coding are described in the following sections.

3.4.1 Open Coding

We began our Grounded Theory process to interpret our data by coding (initial open coding) the data. We created the codes based on the interview transcriptions. We read the interview transcripts line by line and incident by incident and coded them. We kept in mind while open coding that we were looking for patterns and themes. We first kept the granularity of our open coding and ended up creating all types of codes. For example, we first coded Netflix, Amazon Prime, HBO Max, HoiChoi, and Moja Dekho separately. However, in the second round of coding, we minimized the granularity by coding them all under the "entertainment account" code. Some of our codes also came from the discussions where participants revealed beyond what they were asked and shared personal feelings and incidents. For instance, P3 was asked if she shared passwords in her romantic relationships. She also described her beliefs and feelings associated with the sharing.

> *Actually from what ground I shared my password is - I wanted him [boyfriend] to trust me completely. Nothing related to me will be unknown to him. It was something like that. I have never asked passwords from him. Because I believed that every person has something personal. Space is also needed. He also deliberately avoided these issues about sharing. I also felt insecure in my relationship. So I thought if I ask his password or if I force him to give, he might not stay in the relationship with me. These factors worked in that case. I actually never pressurized him with these - even if he did not give passwords, I trusted him anyways. [P3]*

We coded this section as "expression of trust" considering that she interpreted her password as a proof of her fairness in the relationship so that the recipient of the relationship could trust her completely. We also coded this section as "transparency" because she wanted to be transparent in the relationship by sharing password. Lastly, we also coded the same section as "obligatory password sharing" because P3 felt obliged to share the password meaning nobody forced her to share them.

We created 168 open codes. A list of codes and initial categorization is given in Appendix C. We then grouped the descriptive codes by topics like who, what, why, how, how long, how it feels, and so on. By grouping the descriptive codes in this way, we wanted to describe how password-sharing is practiced in Bangladesh. These findings are described in Chapter 4.

3.4.2 Axial Coding

After open coding, we started axial coding. In the axial coding process, we first considered our open codes and looked for patterns and similarities to make a set of higher-level categories. We used Miro to create sticky notes and posted them on the online whiteboard to examine the codes. The Miro whiteboard was shared among the researchers for collaboration. We then looked for connections and patterns among the open codes and then grouped them together. These groups are our initial axial codes. For instance, we were looking for what factors motivated participants to share the passwords with different relationships. It appeared to us that people shared the password when they trusted the recipients or password sharing eased their lives. We found the open codes like "trust", "Depth of Relationships", "Propinquity", and "Expression of Trust" described trust or process of trusting someone to share the

passwords. Participants also mentioned any kind of shared benefits including financial benefits encouraged them to share accounts; therefore, we considered the open code called "Shared Subscription Fees". Participants wanted to help and sometimes wanted to get the help but both of the cases required them to share passwords. We considered both "Help People" and "Technical Assistance" codes in the same group. Lastly, "convenience", "necessity", and "collaboration" also indicated why participants shared their passwords. We decided to group all of these codes together as "motivation of password sharing". We describe our categories in Chapter 5.

Table 3.1: Participants' Information

Participants	Gender	Age	Education	Profession
P1	Female	18-29	UG-2[b]	Student
P2	Female	18-29	UG-3[b]	Student
P3	Female	18-29	Master of Arts	Service Holder
P4	Male	40-49	Master of Commerce	IT Manager
P5	Male	30-39	BBA	Unemployed
P6	Male	30-39	BSc in CS	Screenwriter
P7	Female	18-29	M.Eng.	Service Holder
P8	Female	18-29	Grade-12	Student
P9	Male	30-39	MBA	Hotel Supervisor
P10	Male	30-39	MBA	Service Holder
P11	Male	18-29	Bachelor of Arts	Affiliate Marketer
P12	Male	30-39	M.Eng.	Photographer
P13	Male	30-39	MBA	Businessman
P14	Male	18-29	Bachelor of Arts	Student
P15	Female	30-39	MBA	Service Holder
P16	Male	18-29	H.S.C[a]	Student
P17	Female	18-29	UG-3[b]	Student
P18	Male	18-29	UG-1[b]	Student
P19	Male	18-29	MBA	Banker
P20	Male	18-29	H.S.C[a]	Student
P21	Female	30-39	MBA	Service Holder
P22	Female	30-39	MBBS	Doctor
P23	Male	18-29	BBA	Service Holder
P24	Female	18-29	Bachelor of Social Science	Service Holder
P25	Female	18-29	Bachelor of Social Science	Student

[a] H.S.C = Higher Secondary School Certificate (equivalent to GCE A Level in UK)
[b] UG = Undergraduate (Year: 1, 2, 3 and 4)

Chapter 4

Open Coding

This section reports on our open coding. We coded line-by-line and incident-by-incident. After our initial coding and iterative cleaning processes to modify the granularity of our codes, we ended up having 168 open codes in our codebook (Appendix A). A screenshot of our NVivo interface is given in Figure 4.1.

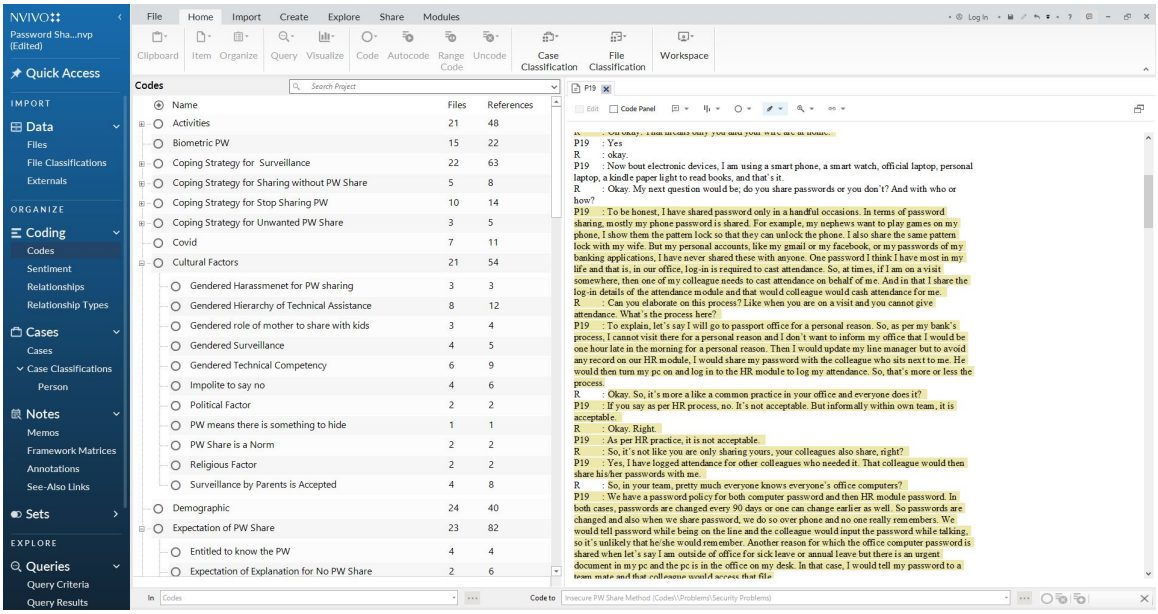

Figure 4.1: Screenshot of NVivo Interface with our coding.

When we further analyzed the codes, we noticed some of our codes described the context, nature of password-sharing, and password sharing processes. We separated such descriptive codes and looked for patterns to group them. We considered the questions like who, what, when, why, how, etc., to explore these codes.

We first grouped the similar codes together with the descriptive group names in NVivo. We then further analyzed each group to understand what question they were answering. For instance, we had some open codes named "Sibling Relationship",

"Parent-Son Relationship", "Parent-Daughter Relationship", "Husband-Wife Relationship", "Other Family" and "Not Family". The first four codes in this example represent the password sharing among relationships mentioned in the name of the code (for example, we coded password sharing between parent and son as "Parent-Son Relationship"). In the "Other Family" code, we coded password-sharing with relationships like cousins, nephews, and uncles. Similarly, the "Not Family" code referred to password-sharing with people other than families, such as friends, colleagues, neighbors, and even strangers. We grouped these five open codes together and named the group "Relationships". We used this group to describe the "who" question, meaning who was sharing passwords with whom. Similarly, we explored what, why, how long, what it felt, and password-sharing techniques to understand password-sharing in Bangladesh.

4.1 Who?

Half of our participants mentioned not sharing passwords in the pre-screening survey. However, during the interview, everyone ended up mentioning password-sharing at some points in their lives. They mentioned sharing passwords in different relationships: family, non-family, and sometimes with strangers.

Passwords were mostly shared in family spaces. In Bangladesh, a *single family* (nuclear family) refers to a family consisting of parents and their children [53]. A *joint family* (extended family) is an extension of the single family where married male children and their families also live in the same household [54]. Our participants came from both single families and joint families. In family spaces, phone/laptop PIN, banking PIN, personal email, entertainment accounts, and social media passwords were shared with spouses, siblings, romantic partners, and sometimes with cousins in case of joint families. Phone/laptop PINs were also shared with children if there were any in the family. Parents usually did not supervise activities and usually did not ask to know the passwords of financially independent male children. Parents sometimes supervised the phone activities and took the passwords of adult children even if they went to university. Earning children might share their banking cards with parents in case they contributed to the household. Participants mentioned that some parents

could not use smartphones; therefore, they sometimes needed the assistance of elder children to supervise the younger ones. Parents were also dependent on their children to use their own smartphones and online banking. Thus, elder or younger children, depending on the availability, created and managed the passwords of smartphones, social media, and online banking accounts of their parents.

Passwords were also shared with non-family members, including close and non-close friends, neighbors, roommates, and colleagues. Phone/laptop PINs, banking PINs, personal emails, entertainment accounts, gaming accounts, and social media passwords were shared with close friends. These passwords could be shared with non-close friends, but if people did, they usually changed their passwords afterward. Neighbors sometimes became friends, and participants mentioned sharing laptop and banking passwords in such relationships. If people lived in a dorm or shared residence, they usually shared rooms with their close friends. In some exceptional cases, people mentioned having roommates who were not (yet) close friends and sharing smartphone/laptop passwords with them.

People did not share their work-related passwords with family members and personal relationships. However, they shared the work passwords with their colleagues, including IT personnel. Sometimes work colleagues became close friends, and people then shared their banking accounts and entertainment accounts with them.

4.2 What?

Our participants mentioned sharing a wide variety of passwords, including banking, email, social media, entertainment accounts, personal and official laptop/desktop computers, and smartphones. They also mentioned performing many different activities with the shared passwords.

4.2.1 Banking PIN

Participants mentioned sharing traditional banking and mobile banking PINs with siblings, close friends, spouses, and colleagues. The main reason for such sharing was withdrawing cash in case of emergency or just convenience. Elderly parents shared their PINs with their (adult) children to assist them in withdrawing money from the

ATM booth or to make transactions online. Romantic partners also reported sharing the banking credentials if one partner faced difficulties making transactions online. One of our participants mentioned sharing her credit card so that her friend/colleague could avail themselves of discounts. Card PINs are also shared to assist friends who are in need of money or with international transactions. One participant mentioned sharing her mobile banking account information so that her friend could buy a train ticket online.

4.2.2 Personal Email

Participants mentioned sharing email passwords with friends and siblings. Email passwords were shared for checking emails or replying to emails back in case the owner did not have the technical infrastructure available to access the email. Participants also mentioned keeping a shared email address for academic collaboration or teamwork. One participant mentioned having a shared email address with friends for making pranks together by sending emails to unknown people. P16 mentioned that his elder sister shares her email password to fix an issue:

> *She [elder sister] trusts me. She says – "I am facing some problems in my email. Here is my password. Log in to my account and fix it or send the email." It happened several times. She shared her passwords with me. Also, she sometimes forgets to log out [from P16's laptop]. [P16]*

Participants also mentioned that they created and managed their parents' email credentials. Email addresses were required for using smartphones; however, the parents did not typically have any email accounts. Therefore, the participants usually opened and managed the email addresses and configured the smartphones on their parents' behalf. One participant mentioned doing the same for his wife, and she also did not know her email password.

4.2.3 Social Media Account

Social media passwords were primarily shared in romantic relationships and with friends. Participants mentioned checking what the partners were doing on social media both secretly and openly. P5 mentioned a secret surveillance scenario:

> *My girlfriend gave me her [Facebook] password later. After she gave me her password, I did check without her permission towards the end of our relationship. I just wanted to see whether she is backbiting with my friends or what she is doing. I used to go through her chats logs and everything, but I did not inform her about this. Fortunately, she did not do anything, so I am good (laughing). I did not change anything; I just spied on her. If I had changed anything, I would get caught because she knew I only had the password. She is smart, right? She would definitely know that I am spying on her.*

Participants also mentioned sharing their Facebook passwords with partners/close friends so that they could upload photos or statuses on their behalves. Also, participants mentioned sharing Facebook passwords with siblings and close friends to fix any problems there on their behaves (for example, account compromise). Participants sometimes created and managed the social media accounts of their parents.

4.2.4 Entertainment Account

Entertainment accounts, such as Netflix, Amazon Prime, Hoichoi, etc., were frequently shared among friends and family. The main reason for sharing entertainment accounts with friends was to split the subscription fees. Sometimes participants also shared these accounts with friends only because their friends wanted to watch any particular show available there. Participants also mentioned sharing shared entertainment accounts with romantic partners and siblings. For instance, when participants shared Netflix accounts with friends to split the subscription fees, they also shared the passwords with their wives or brothers.

4.2.5 Personal Computer

Personal computer/laptop passwords were usually shared among siblings and friends. Participants were found to share their PCs with siblings if that was the only computer available in the household. PC password recipients usually watched movies, attended Zoom classes, submitted assignments online, used social media, browsed on internet, checked/replied to the emails, finished official work, and bought something online. One of the participants mentioned that he had a powerful laptop that supported demanding software, and his friends borrowed his laptop to use that software.

4.2.6 Smartphone

The smartphone PINs were shared with parents, friends, siblings, spouses, and romantic partners for various reasons. One of the most common reasons for such sharing was for making calls. Parents also could demand the passwords of phones for surveillance. Elder siblings, spouses, and partners also took the passwords for surveillance. Friends and siblings took the passwords to take photos, check the photo albums, and listen to music. Sometimes, the younger siblings took the phone to play games and watch online videos. It was also common to take parents' phones by the children for playing games and watching videos. Participants also mentioned sharing their phones with friends who did not have phones to access their social media accounts.

4.2.7 Work Devices

Participants did not share their work laptop/desktop passwords with family members. They also did not share work phones with their family. However, they frequently shared work passwords with colleagues. The recipients usually performed different work-related tasks with the shared work password, including accessing files, checking/sending work-emails, printing work-emails, giving work attendance, and updating information in the enterprise resource planning (ERP) software.

4.3 Why?

People shared passwords for several reasons in different contexts. Based on the data provided by our participants, we identified two settings for sharing passwords: voluntary password sharing and obligatory password sharing.

4.3.1 Voluntary Password Sharing

Voluntary password sharing refers to when people, by their own choices, shared their passwords. People voluntarily shared their passwords because of convenience, shared benefits, and necessity.

Password sharing gave convenience in regular lives. People sometimes relegated and distributed tasks that required sharing passwords with other family members.

For instance, financial contributions by spouses, parents, and adult children were managed by password sharing. The younger members of the family also got hold of such financial money to perform tasks like withdrawing passwords or shopping for the family. Participants also voluntarily shared their subscription-based passwords, for instance, entertainment accounts. P9 described why his friend voluntarily shared his Netflix password:

> *He then proposed me that if he pays it [Netflix account] all by himself then he would have to pay 1000 BDT per month but if we share among our four friends, it would just be BDT 250 per person. So, we three friends then joined him and he shared the credentials. [P9]*

People sometimes just needed to share their passwords for some specific work to be done in some unavoidable situations. We are considering here those situations when the tasks could not be done without sharing passwords. For instance, P25 went to visit Bandarban (a remote hilly area in Bangladesh), and all of a sudden, she had to send her resume urgently. She did not have an internet connection there. In such a scenario, she shared her email id and password with her best friend and instructed her to send the resume. Unavailability of mobile networks, the internet, and devices and inability to operate the services were the roots of such necessity-based sharing, and people then voluntarily shared the passwords.

4.3.2 Obligatory Password Sharing

Obligatory password sharing refers to when people shared their passwords by feeling obliged or forced to share. The main reasons for obligatory password sharing were trust, responsibility, and coercion. Participants felt obliged to share their passwords with family members and romantic relationships because they were supposed to trust these relationships. Password sharing symbolizes an expression of trust – if someone shared the password with somebody, it meant that they trusted them. However, sometimes they also felt forced to share the passwords. For instance, sometimes participants did not feel right sharing their mobile laptop passwords with their siblings – but they had to share anyway because sharing devices was necessary for their family role. In this kind of sharing, participants usually monitored the activities by sitting beside those they had shared with or hid personal data. Participants mentioned

sharing their mobile passwords with parents or elder siblings because they forced them to do so. In such cases, participants' activities were usually under surveillance by the parents or elder siblings. For instance, P3 mentioned that her parents used to seize her mobile phone when they became aware of her boyfriend. P22 was not allowed to lock her phone because her mother would check whether she was having a romantic relationship or not. P11's mother also knew his mobile phone's password when he was in college, and he had to show his phone whenever his mother demanded. Participants mentioned keeping two mobile devices (one hidden from the family) and two memory cards to cope with such coercive password sharing.

4.4 How?

Participants mentioned sharing passwords following two methods: verbally and in written form.

4.4.1 Verbal Password Sharing

Participants usually shared passwords verbally. Participants mentioned two types of verbal password sharing: in-person verbal password sharing and on-call password sharing. In-person verbal password sharing happened in case of proximity; therefore, it usually happened in family space. People shared their phone and laptop passwords, banking passwords and entertainment passwords in-person verbally with their spouse, parents, siblings and children. For instance, P1 shared her Netflix password verbally in person with her sister because she lived with her in the same household. Roommates also shared their passwords in-person and verbally.

Participants shared the passwords over the phone if they were not near the device or to the recipients. For instance, P19 shares his password in the workplace over the phone. He mentioned the process of sharing in such a scenario:

> *When we share passwords [with colleagues], we do so over the phone, and no one really remembers. We would tell the password while being on the line, and the colleague would input the password while talking, so it is unlikely that he/she would remember. Another reason for which the office computer password is shared when I am outside of the office for sick leave or annual leave, but there is an urgent document on my pc, and the pc is in the office on my desk. In*

> *that case, I would tell my password to a teammate, and that colleague would access that file. [P19]*

In case people did not have any internet connections but had phone services, then they shared their passwords over the phone with friends to take care of any necessity. For instance, P6 mentioned that his friends living outside of Dhaka city (having limited access to internet) used to call him and gave the email IDs and passwords to fix some of the problems with their email accounts in early 2000 when internet was scarce outside of Dhaka.

Even if people knew the passwords but the accounts were two factor authenication (2FA) protected, then the owners had to share one time passwords (OTP) over the phone in case the recipients were not near to them.

4.4.2 Written Password Sharing:

People shared written passwords either by writing them in online chat or in email. Writing in chat was more common for our participants. Writing passwords occurred if the accounts could be accessed from anywhere and the recipients were not near the participants. Most of our participants who shared their Netflix with friends mentioned sharing passwords using chat or emails. If the passwords were shared in chat, it was hard for the participants to find the passwords later. In case they needed the passwords again, they usually had to ask the owner. It was quite easy for the participants to find the passwords shared by emails. As P4 mentioned:

> *He [friend] shared me [Netflix account passwords] in my Gmail. I remember it clearly because if I forget this password, I go to Gmail to check it, and then I log in [using the password]. [P4]*

People also share their online banking credentials using chatting platforms.

4.5 How Long?

People shared passwords for different spans of time. We have identified three types of password sharing based on how long the passwords were shared: temporary password sharing, ongoing password sharing, and hybrid password sharing.

4.5.1 Temporary Password Sharing

Temporary password sharing means when passwords were shared for a limited amount of time and password sharing was terminated after the task was done. Temporary password sharing occurred in several contexts. For instance, passwords were shared temporarily with people with whom the relationship was not close, but the passwords had to be shared by necessity. Accounts like email, social media, online banking accounts, and phone PINs were usually shared temporarily. People usually terminate password sharing by changing the passwords. One example of temporary password sharing is when P4 had to share a sensitive work password with one of his co-workers, but he changed the passwords as soon as he got the internet connection back.

4.5.2 Ongoing Password Sharing

We define ongoing password sharing when people kept sharing the passwords for an undefined time. This kind of password sharing happens with the trusted people: family members and close friends. People shared their phone, laptop, banking, email, social media, and entertainment account passwords with close friends and family members. Ongoing passwords were usually shared in written forms so that the recipients could access the account even if they forgot the passwords. In the subscription sharing model, passwords were shared on an ongoing basis, even with non-close friends and strangers. For example, P23 mentioned having password of a Netflix account which was actually shared by his brother and his brother's friends.

4.5.3 Hybrid Password Sharing

We define hybrid password sharing as when the password sharing could be both temporary and an ongoing basis. For example, when people shared the passwords of physical objects like banking card PINs, smartphone PINs, and laptop PINs, they did not need to change the passwords to terminate the sharing. Instead, they had to get hold of the devices to end it. For instance, P5's ex-girlfriend knew his phone's PIN. When the relationship ended, he did not change the PIN because she would never get hold of the phone. Similarly, Wi-Fi passwords and printer passwords required proximity to the devices, and the access terminated with the distance to the devices.

Therefore, these types of password sharing could be both temporary and ongoing. If the devices were in the same household and could be accessed unattended, it would be considered as ongoing password sharing. For instance, the Wi-Fi password in the household: when it was shared with the family members, then it is ongoing password sharing. However, if the passwords were shared with people who did not live in the same household, then sharing would be considered as temporary password sharing. For instance, if the Wi-Fi password was shared with relatives who came to visit for a short period of time, then it was temporary password sharing.

4.6 Password Sharing Sentiments

Our participants experienced both positive and negative feelings when they shared passwords with different relationships. When participants talked about their positive feelings, they mentioned feeling comfortable, not obliged and unconcerned to share their passwords. However, participants also felt uncomfortable, concerned, fear, regret, and obliged for sharing passwords in some contexts.

4.6.1 Positive Feelings

The majority of the time, participants felt good about sharing passwords. We noticed their satisfaction when they voluntarily shared their passwords. Some positive feelings that our participants felt related to password sharing are described below:

Comfortable: Participants felt comfortable sharing passwords with some people because of the depth of those relationships. P1 described her feelings when she shared her mobile phone and card PIN with her best friend:

> *If I must describe more precisely, I did not actually feel like it [password sharing] was a violation of privacy. She is my best friend, and I am very much comfortable with such sharing with her, and that is why I shared my password. [P1]*

In Control: Participants mentioned that they felt good when they shared passwords because they were not forced to share. Instead, they willingly shared their passwords to help or get help. Both of the cases made them feel positive about password sharing. P2 shared her email credentials with her friends so that they could

submit assignments on her behalf when she did not have internet access. She felt very positive about this sharing because it brought convenience to her life. She also shared her entertainment account with her best friend voluntarily so that her friend could watch animes. She described her feelings:

> *I mean, I felt like I needed to share the passwords; that is why I shared. It is not like I am obliged to, or I would have to share. [...] As I told you before, my friend uses my Crunchyroll [Anime streaming site]. She wants to watch animes there. That is why I shared. She has her own accounts in some other streaming sites where she watches anime. However, not all sites premiere all animes. So, in that case, I felt like I could give my Crunchyroll passwords so she could watch some animes that are not available on the sites she uses. It is not like she is forcing me – you have to give me or blah blah. It was not like that. [P2]*

Unconcerned: We also noticed some participants were not concerned about sharing passwords in some contexts. They did not foresee any harm from password sharing; hence, they felt relaxed and not worried about it. P19 mentioned his positive feelings about password sharing:

> *About my phone, there is one pattern lock to get into my phone. I have kept that pattern lock very simple. My wife knows it, and my two nieces know. Also, for an incident, my line manager at work needed to use my phone for something, then instead of me unlocking the phone for him, I just gave him the pattern to unlock. So, he knew, and honestly, I never really changed my password afterward. I am not really concerned about this one very much. I am not very bothered that someone would take the trouble of getting his hand on my phone and would take some sensitive stuff or do something weird. So, these people know my pattern to unlock my phone. About Wi-Fi password, my wife knows, and then if a guest comes over, I share my Wi-Fi password without hesitation. [P19]*

4.6.2 Negative Feelings

In general, participants felt some negative feelings when they performed obligatory password sharing. Feeling fear, discomfort, and obligation were commonly mentioned as negative feelings for obligatory password sharing. Some participants also mentioned that they regretted voluntarily password sharing because they had to face unexpected bad consequences.

Discomfort: Our participants mentioned feeling uncomfortable sharing passwords because of a lack of depth in relationships with the recipients of the passwords. For instance, P1 was comfortable sharing her phone password with her best friend in university. However, she felt uncomfortable sharing the same password with her classmates in some contexts, for instance when she had to share her phone's PIN for taking photos together. She was also on good terms with her other friends, but she still felt uncomfortable because the relationships were not so deep as to feel comfortable about it. On the other hand, participants trusted their parents unconditionally but sometimes they felt uncomfortable sharing passwords with them because they would not approve of some activities, such as having romantic relationships or friendships with the opposite gender. P17 felt uncomfortable sharing phone with her parents because they were not "liberal" enough to accept some of her activities (e.g., having a boyfriend); therefore, she always remained "vigilant" about her private data. P15 described her feelings:

> *I feel some sort of uncomfortable when I share [phone/password] with parents; for instance, my chat box is open, and my phone is at my father's hand. However, I have never taken any measure for that (laughing). [P15]*

Sometimes participants felt uncomfortable in case someone saw their online activities because of password sharing. Participants mentioned such feelings when they shared their entertainment accounts. There was discomfort because the other users with whom the passwords were shared might see watch-history and judge them for their movie choices. For instance, P23 used Netflix, which was shared with his brother and brother's friends, and he explained his discomfort about it:

> *It does come in my mind that - did anyone see what I watched? I know it does not matter, but still, I would like to keep things private. But then, no one will know who is watching it since there are four users. If it were shared between only me and my brother, I would feel more uncomfortable because then if he has not watched anything, but it is there on the home page, he would know that I am the one who watched it. [P23]*

Religion and hijab wearing were critical to some participants, and they mentioned feeling uncomfortable for the possibility of their non-hijab photos getting seen by others. P25 wore hijabs, and she described her feelings:

> *My chat history and everything is not really my problem. My main concern is that I wear hijabs, and my close friends are always curious about how my hair is, how long it is, and all, and I am not at all comfortable showing them any picture without my hijab. So, whenever someone, be it a kid coming to our home or my friends access my phone, I get nervous thinking they can see my pictures without a hijab if they go to my photo gallery. So, whenever I see that someone is trying to access my gallery, I would make up an excuse like I need to check something urgently and immediately take back the phone. I do not usually give the phone back. [P25]*

Fear: Participants also mentioned having stronger feelings like fear when they shared passwords. They feared of the awkward situations and the possibility of losing access or money from password sharing. For instance, P17 was having a romantic relationship which she hid from her family. She described her fear of any awkward situation that might occur because her elder sister knew her password:

> *I sometimes think about it. For instance, I am talking to my friend about a secret or something, and suddenly my sister came and saw the conversation, and I may fall into an awkward situation. I sometimes feel like whether I should enable the Bio-metric of my phone – but I forget to set it up. It happened, and I sometimes get tensed about whether she sees something in the middle of a conversation. I do fear that sometimes. But nothing yet happened so far – no awkward situation arose yet. That is why maybe I am like, "damn care" (laughing), but I cannot think of the day if something like this happens! I actually need to change my password. [P17]*

Obliged: Participants also felt forced at times to share their passwords. The majority of the participants mentioned that it was a familiar phenomena and culturally expected to share social media passwords with their romantic partners. Surveillance by the partners was also expected in both marital and pre-marital romantic relationships. Not all of our participants felt positive about this type of password sharing. Not sharing was not an option either, because it would cause questions like trust issues and commitment. For instance, P5 gave his social media password to his girlfriend because he wanted to show that he had nothing to hide – but he was not happy with the sharing. P6 described the feelings that some of friends shared with him related to password sharing:

> *They [friends] say that they had to share their passwords with their wives, and it was kind of mandatory. It is because people have trust issues. I have never faced such a problem. Some of my friends lock their phones, but they had to*

> *share the PIN with their wives. I heard them complaining about why they had to share it (laughing). This is a very common practice here. [P6]*

Regret: If the password recipients behaved unexpectedly or the password sharer had to face any extra hassle caused by sharing passwords, then participants mentioned regretting their voluntary password sharing. For instance, P25 shared her mobile banking account with her friend voluntarily to help her, but she lost access to her account for a considerable amount of time for this sharing. Such hassle made her regretting the sharing. As P25 described the situation:

> *I did not have much money there [mobile banking account], but I still had some. But you see that your account - which never showed an error message before, suddenly is not letting you even enter the account. At that moment, I really regretted sharing my password. I kept thinking that even if it were to be painful to say no, I should not have shared the password. I thought that I would not be able to recover my account. [P25]*

4.7 Password-Sharing Techniques

Our participants sometimes took precautionary measurements when they shared passwords to protect their private information from surveillance and to have control of the shared accounts. Techniques for protecting private data and secrets in shared accounts repeatedly came in almost all of our interviews. Sometimes, participants were also found to take measures to control what could be done with the shared accounts, including when to terminate the sharing. Some common strategies are described below.

4.7.1 Lock Private Data

Most of our participants considered their photos were private data. To protect a photo gallery of phones from surveillance, participants used application locking software, for example, Photo Vault and AppLock. Participants who used the app locking applications did not share their app lock password with anyone. Parents of our participants were not tech-savvy and usually did not realize that the photos were locked even though they had the phone PINs. Spouses of the participants noticed the lock

and asked to know what was there. Participants usually showed the gallery by unlocking the app but did not share the passwords. In shared laptops/PCs, participants locked the drive or folder to keep their files secret. P12 mentioned his reasoning for password-locking files:

> *Since he [younger brother] is young, he might have curiosity over my belongings. This is very normal. He can be like – let us see what Bhaia [Bengali word to call elder brothers] keeps in C drive. So, I locked some drives. [P12]*

4.7.2 Delete Private Data

Deleting personal data was a commont practice among our participants. Some of our participants mentioned not keeping photos in the phone-gallery and deleting them from the fear of surveillance. The personal photos were critical, and it mattered to participants what other people thought about them if they saw them keeping some photos. P12 explained why he deleted some of his photos and kept selected photos in his phone gallery:

> *My phone is really personal. I actually personally categorized what to keep and what not to keep on my phone. I do not keep anything in my phone in case the phone gets lost, or my friend asks for it – I mean, if my friend asks for my phone to call, I will definitely give them my phone. They can check my photo gallery as well. These things can happen anytime, and I cannot say they will not happen ever. People usually go to the gallery, and that is why I do not keep anything there. I delete what I do not want to keep. Basically, I keep what represents me. [P12]*

Participants in romantic relationships were aware of surveillance by their partners. They sometimes deleted conversations of their friends to keep them hidden from their partners. For instance, P15 used to delete some conversations with her friends on messenger and WhatsApp before going on a date. She thought her boyfriend would ask some questions if he saw the conversations, and she wanted to avoid them. P3 explained herself why she deleted some chat conversations before going on a date:

> *I was in a relationship with him, and there was not anything that would create a problem if he knew. There was nothing to hide. But it was mostly my chat with my female friends [that I deleted] because he might get hurt seeing those.*

> *In reality, we maintain a different level of relationship with each individual. We do not talk similarly with everyone. So, I have a relationship with my friends for seven years. When I talk to them...it's like...they are almost my family. On the contrary, my relationship with my boyfriend was only for two years. From that perspective, I felt like there was something completely personal. It's not like I would have to tell him everything. [P3]*

Participants also deleted photos and contents to protect their privacy from parents' supervision. P15 used her parents' phone to communicate with her boyfriend and used deletion to hide her activity trace:

> *I always had a phone. I mean, once, we had to use our land phone, but that was a long ago. Umm...I also used my parent's phone (to call my boyfriend) when I did not have any personal phone to make a call. He [boyfriend] knew that it was my mother's number or my father's number. I did not take any precautions but just deleted the number from history after calling. [P15]*

Participants also deleted their photos and chats because they shared phones with their parents. P3's parents did not accept her relationship, so she used to delete all of her relationship-related data including photos, chat history, and text messages. P8 also deleted any "friends only" photos shared in his WhatsApp:

> *My friend sent something like a funny picture with me on WhatsApp, and if my parents saw it, they might get offended because they are old. So I deleted the photos. [P8]*

4.7.3 Hide Private Data

All of our participants hid their private data following different methods. Almost all the participants had hidden folders where they kept their personal photos. Password protected folders created questions like what was there or what they were hiding there, but hidden folders saved them from such questions. P4 was an IT manager, and he both encrypted and hid a drive to keep his personal data.

> *There is a drive where I kept photos of my friends, which is completely hidden. Only someone who is technically knowledgeable like me will understand its existence and find it by asking questions like where is that 200 GB of space. General people will not understand such things. [...] I use software to encrypt and hide the entire drive. [P4]*

Participants also mentioned disguising phone contacts using false names. For instance, P3 was not allowed to have a boyfriend, and she hid his contact details:

> *I did not keep anything related to my relationship in my phone. I deleted my chat histories. I did not even save his number with his original name. I saved that with a female friend's name (laughing). So even if my phone was checked suddenly, I could remain safe. [P3]*

4.7.4 Multiple Devices and Accounts

Some participants mentioned keeping multiple devices, memory cards, and accounts to protect their private data. For instance, when P11 was in 12th grade, he kept two memory cards – one was to show publicly to his mother and another one was for keeping private data. In P11's words:

> *I managed my privacy following different methods. For instance, the things that she [mother] should not see or know, and I deleted them. I also tried to keep my private data separate. For instance, there was a picture that I did not want my parents/family to see. Then I used two memory cards – one for keeping these hidden photos and the other for publicly showing – see, I only have these things here – I have nothing to hide! I mean, I dealt with it based on the situation. It was easier for the PCs; I created a guest account and let others use and check that one and forbade them to use the one with my name on it. I also practice this now. When people come to my place, they use the guest account. [P11]*

Multiple participants mentioned having guest accounts on their PCs and laptops. Sometimes participants lent their laptops to friends, and having two accounts eased their lives. Participants sometimes kept two smartphones – one of them was kept hidden from the family. P3 used Tinder and she did not want her friends and family to know about it. So she kept two phones – one for Tinder and personal data and was kept hidden from everyone. Another phone was for publicly sharing, for instance, sharing with siblings and friends.

4.7.5 Monitor Activities

Our participants sometimes monitored the recipients of their devices so that they could not perform any unwanted activities (e.g., checking photo gallery, messages,

etc.). When participants felt a bit uncomfortable sharing their devices, they usually stayed beside the recipients, monitored what they were doing, and took the phone back right after the task. Monitoring was practiced widely while sharing with friends so that they could not check the photo gallery. Some participants also practiced monitoring with their parents. P15 described her attitudes while sharing smartphones with her parents:

> *I would feel a bit uncomfortable like I am sitting there and they [parents] are talking with someone using my phone. I would just stay in front of them so that I can see whether they are checking my phone or not – to be precise; I would take the phone away before they start checking (laughing). [P15]*

P9 mentioned keeping a log when he let his colleagues use his office PC. In his own words:

> *Even though I feel uncomfortable, I have to share the password sometimes [with colleagues]. To be on the safe side, after they finish the task, I change the password. Also, the software I am currently working on can take a log on a time basis. So I sometimes take logs of the period that I share my password with my colleague. I could see the changes that they have made. To be on the safe side, you know? I can take a screenshot – what changes were made during that time. [P9]*

4.7.6 Other Strategies

There were some other strategies of password sharing that were not widely practiced but came during our interviews. For instance, participants mentioned that they did not save their banking cards in their e-commerce accounts if the account is shared. Therefore, even if the account is shared, the password recipient would not be able to purchase something using the owner's card.

In some romantic relationships, participants shared their Facebook passwords with their partners. They made their close friends aware of such Facebook password sharing and forbade them to write anything private there. They used other platforms, such as, WhatsApp, for communication.

Some of our participants shared their phones with younger members of the family so that they could play games or watch videos. Participants mentioned turning off

the notification of their messengers/messages so that the children could not get the pop-up notice and accidentally read the message.

Chapter 5

Axial Coding

Axial coding was the second phase of our qualitative data analysis. In this phase, we assembled our large set of open codes into conceptual categories. We first created online sticky notes on Miro with the names of our open codes. We then moved the notes around the board, trying to group them together. During this process, we wanted to find connections between our codes. A screenshot of a portion of our Miro Board is shown in Figure 5.1.

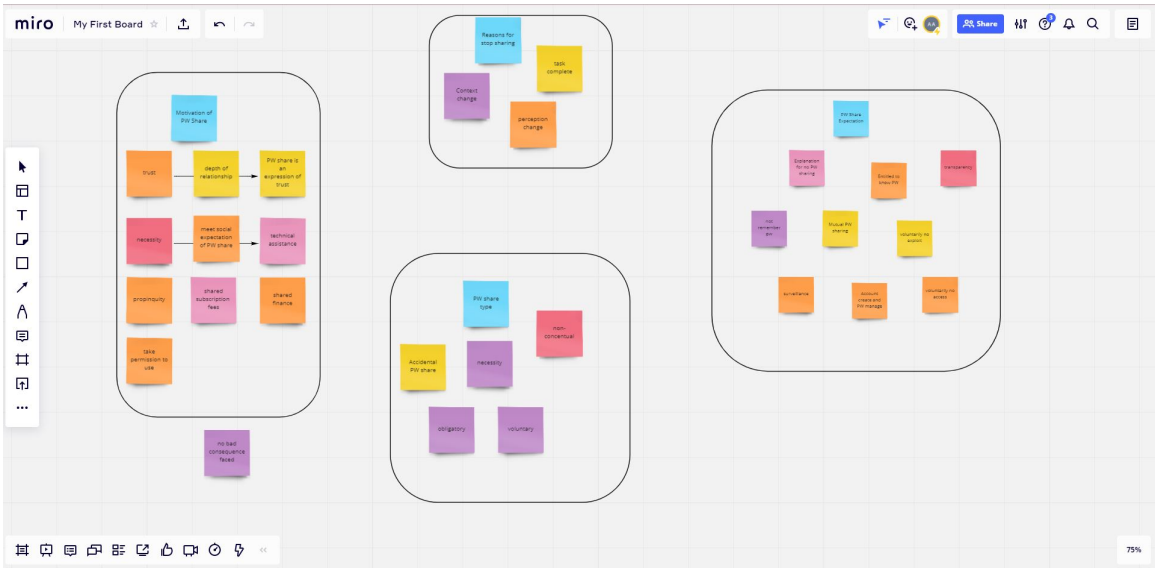

Figure 5.1: Screenshot of Miro Interface where we categorized our open coding.

We read through the open codes and tried to find patterns and common phenomena among the open codes. For instance, we had open codes named “Gendered Harassment of PW sharing”, “Gendered Hierarchy of Technical Assistance”, “Gendered Role of Mother”, “Gendered Supervision”, “Impolite to say No”, “PW Share is a Norm”, “Surveillance by Parents is accepted”, “PW means there is something to hide”, etc., which we put together. We then re-read the quotes from these codes

and observed that our participants mentioned some beliefs and practices related to password sharing that were rooted in their cultural context. We created a category named "Cultural Factors" with a different colored sticky note and grouped these open codes together. We also created the "Cultural Factor" category in NVivo and nested the open codes under it. We removed some open codes after reading the quotes of our grouped open coding. For instance, one of our open codes was "Power Relation between siblings" where we coded the situations where elder siblings exercised power over younger siblings, or younger siblings felt the power of elder siblings in terms of sharing passwords. After reading the quotes, we realized that there was no cultural component there, and we removed it from this category. Similarly, we had an open code named "Political Context" and we added this code to our "Cultural Factor" category after re-reading the quotes.

We followed the same process for the rest of our open codes. While trying the group the rest of the open codes into categories, we came up with few categories like "Motivation of PW Sharing", "PW Sharing Expectation", and "Problems with PW Sharing". Our further analysis resulted in finding a pattern between these categories that they depicted different stages of password-sharing sequentially. We structured them together linked by an axis indicating the sequence of stages.

These two categories as mentioned above are the major axes of our analysis: the first is the "sequence of stages" in the password sharing experience, and the second is the "cultural forces" that affect that sequence.

In the following sections, we first describe our axes in Sections 5.1 and 5.2. In Section 5.3, we describe a theory refined from our axes, relationships, and patterns.

5.1 Stages of Password Sharing Experiences

5.1.1 Motivation of Password Sharing

We have identified four factors that motivated our participants to share their passwords: trust, necessity, convenience and collaboration. One or multiple factors worked to motivate people to share passwords.

Trust: According to our interviews, one of the primary motivations for sharing

passwords involved trust. Trust played a complex role in whether passwords would be shared or not. All the participants mentioned that they shared passwords with family members, including parents, siblings, children, partners, and spouses, and with some non-family members like friends and colleagues because they trusted them. After analyzing the data, we found the existence of mutual trust among family members, the depth of relationships indicated the level of trust, and people usually trusted IT personnel of their offices with their work related passwords.

All the participants mentioned that they trusted their family members with a variety of passwords. We noticed the existence of mutual trust – everyone in the household trusted each other unconditionally that family members would not cause any harm. However, participants mentioned trusting different passwords with different relationships. For instance, adult children might trust their siblings with their social media accounts, but they would not trust those accounts with their parents fearing surveillance. However, our participants mentioned the existence of mutual financial transparency among family members – almost everyone trusted each other with their banking credentials and shared them in case of necessity. Wi-Fi passwords and entertainment account passwords were also shared in the family space. Parents trusted their children with their phone and laptop passwords. Adult children in the family trusted their phones with their parents and siblings; however, they also hid contents, following different methods.

We noticed that the level of trust depended on the depth of the relationships. The highest level of trust is what participants felt for family members. Sometimes, participants mentioned trusting some non-family members, such as friends, roommates, and colleagues, at the same level as family. For instance, participants described their friends, roommates, and sometimes colleagues "best friends" or "like a family" when asked to explain why they shared the passwords with them. We found a few factors that increased the depth of the relationship. For instance, the length of a relationship determined the depth of relationships. Childhood friends were trusted like family because they had been friends forever. Similarly, one of the main reasons for not sharing passwords with romantic partners was that the relationship was short and did not reach the point of sharing passwords. Another factor that increased the depth of

relationship was the *propinquity effect* - the tendency of forming trust for the people with whom they live or encounter often. Participants mentioned trusting people with their passwords because of the nearness to some people. For instance, in joint families, people put similar trust in cousins or nephews/nieces as they would put in siblings. Similarly, parents also trusted their nephews/nieces living in the same household for technical assistance - similar trust they had for their adult children. Participants also mentioned trusting roommates because they spent a lot of time together in the same household. In the office environment, when people spent the majority of the time of a day with certain colleagues there, the relationship might develop to the highest level of trust. P19 explained his relationship with colleagues:

> *And about trusting my office colleagues is because they are now like a family to me. Also, someone from the office will not be able to flee away after doing something unlawful. So, that factor also works in my mind. Plus, I know the background of each co-worker, their family, what kind of family they belong to, social status, everything. So, all these factors contributed to trust them. [P19]*

Our participants mentioned a tendency to trust IT people with their official passwords. Most of the time, they did not have a deep relationship with IT; however, they trusted them with their official passwords because of their credible work title. People usually did not change their default set up passwords knowing those passwords were set by the system administrators. If participants faced any problem connecting to a video conference while working remotely, they mentioned sharing passwords with IT personnel to check the problems. P4 [IT manager] mentioned that there existed an official rule at his workplace that employees had to inform him of any kind of password changes. He saved all of their passwords and accessed their accounts in case of necessity (e.g., if any employee was absent). He also mentioned that all the employees complied with this official policy. His superiors also sometimes trusted him with their personal email passwords and instructed him to remember them on their behalves.

Necessity: People also shared passwords when there was any necessity. One of the major necessities was providing technical assistance to parents, siblings, spouses, and friends. Participants mentioned knowing the online banking credentials of parents/wives because they did not know how to create accounts there. They also knew

the email and social media ID and passwords for the same reason. P19 mentioned how his parents used digital accounts:

> *My father and mother cannot use digital devices completely. So their digital devices, Facebook, messenger, and even their bKash account are opened by me. So I actually know each and every password. [...] Umm...actually...my father knows the password of the bKash app. They do not know the other passwords. Everything is auto logged in. Passwords are saved there. They use these in this way. [P19]*

Sometimes elder siblings helped those younger to open Facebook accounts. If the accounts got hacked, or problems arose in social media or email, people either shared the passwords with siblings or friends to fix the problem.

Another kind of necessity was when a service was not accessible without password sharing. For instance, participants mentioned that parents/siblings/friends shared bank cards and PINs if they could not go out to withdraw cash. Such necessities could come in different forms. For instance, if participants were out of internet connection and needed to submit assignments, to reply to an emergency email, or to send any official documents, then they shared passwords with friends or colleagues. Younger siblings who did not have smartphones or laptops used elder siblings or parents' devices for attending online classes, calling friends, submitting assignments, and using social media. Among friends who did not have smartphones or laptops, they sometimes borrowed friends' devices to make calls or use a particular software.

Convenience: Participants also shared their passwords for convenience in their lives. We define convenience when the sharing is not a necessity (there were workarounds without password sharing) but sharing passwords made the situation easy and beneficial. For instance, P12 felt too lazy to go to the ATM booth sometimes and sent his younger brother with his card and PIN to withdraw cash. In his words:

> *I would have gone by myself [if password sharing was not an option] to withdraw cash from ATM. I would not be that lazy. It is not like I cannot do that work myself. Since I have this option now – I make him [younger brother] do it – he is very young so he listens. So because of my lazyness, I am sharing my password. But I could do it by myself. I do not think password sharing is necessary. [P12]*

P7 and her husband shared passwords of their banking cards so that they could skip the hassle of distributing the finance of day-to-day lives. If the father and elder son were the earning members of the household, they also shared the banking PINs and cards with each-other. Shared subscription fees by password sharing also brought financial benefits in participants' lives. Friends shared their entertainment accounts (e.g., Netflix, Amazon Prime, Hoichoi, etc.) with friends so that they could split the subscription fees.

Collaboration: Participants also mentioned that they shared passwords to ease collaboration or teamwork. These kinds of attitudes were seen mainly in academia, offices, and in close friendships. Participants mentioned opening an email account and sharing the credentials with the other group members of any academic project. They also mentioned not accessing the account after submitting the assignment. Sometimes, people needed to share access to the "official" desktop so that other team members could work on their portion of the task. As P9 mentioned how it was practiced in his office:

> *I am talking about my company – I finished some tasks and now I will pass it to the next person to finish his/her task. For instance, I did that task using my desktop but I did not pass it to the other person – I am absent or I am out of office that day. But they needed to finish that task. So I would give them my password and mention where the task is and requested him to finish from there if I knew I would not be there on the next day. This type of sharing happened many times. [P9]*

Participants also mentioned sharing the passwords of gaming platforms so that they could play together. One participant mentioned having a shared email account with friends using which they sent prank emails to random people.

5.1.2 Expectations for Sharing Passwords

When participants shared their passwords with different relationships, they usually had some unspoken expectations about how the recipients would use the passwords. So, participants shared their passwords, believing that the recipients would act accordingly. On the other hand, the recipients also had some expectations, which explained why they thought passwords should be shared with them. The expectations also varied based on the account type and with whom passwords were shared. This

section will discuss some of the expectations from both the sharer and the recipient's point of view.

Expectations of the Password-Sharer

When the sharers shared their passwords, they usually expected that the recipients would not harm them and afterwords would voluntarily forget the passwords. Sometimes, especially in romantic relationships, the sharers expected their partners to share the same passwords when they shared theirs. We termed such mutual password sharing as *reciprocal password sharing*. Also, surveillance by parents and partners was widely expected by the sharers.

Voluntarily No Exploit: When participants shared passwords with family and non-family relationships, they mainly expected the recipients would not harm them or voluntarily access personal data. Such expectation was also connected to the level of trust that they had for the people they shared their passwords with. In family space, participants expected parents, spouses, and sometimes elder siblings to invade privacy both openly and secretly in some contexts. However, they usually expected their siblings not to invade privacy when they shared their devices and accounts. P16 described his expectation when he shared his laptop passwords with his elder sister:

> *When my [elder] sisters were not married, they would ask me to unlock my phone if they needed to call somewhere. It is also the same for my laptop. I would unlock the laptop, and they would work there. Also, if Apu [Bangla word to call elder sisters] comes home these days and needs to work on a laptop, I verbally tell her the password, and she uses it. But she never looked into my stuff. She had never done it...she does not [emphasis]. At least no one in my place does that. [P16]*

When the password was shared with non-family members, the expectation remained quite similar: the recipients would respect privacy and not look into private data. For instance, P20 shared his laptop passwords with his roommates, and he described his belief in the interview:

> *They [roommates] know my laptop password as they at times use mine. I also know theirs. They at times need to work on Photoshop, which requires a powerful laptop, and I have let them use mine. I also sometimes download movies that they watch on my laptop on their own. About my digital life on*

my laptop, I don't think they ever accessed anything, and I also never felt the need to say anything. [P20]

Voluntarily Forget Password: Participants also sometimes expected that the recipients would forget the passwords after the tasks were done. These types of expectations were for both family and non-family members. For such expectations, participants usually did not change the passwords after sharing. In the family context, device passwords like smartphones and laptops were sometimes shared spontaneously. P21 described a spontaneous situation and her expectations related to the sharing:

I use a fingerprint [to unlock phone]. Only a handful of times think I had to ask my younger sister to unlock it using the PIN because my hands were busy, but I do not think she remembered the PIN. A similar thing had happened with my parents too on and off, but none remembered each other's passwords, I think. [P21]

Similarly, participants also expected the non-family recipients to forget the passwords after the tasks were done. It was overly seen in the context of work password sharing. Sometimes when participants did not go to the office but needed tasks to be done from their office desktop, they usually shared their credentials with their colleagues to finish the tasks on their behalf. Participants believed that their colleagues would forget the passwords after finishing the tasks. They did not change the passwords until it was required by IT. Some of the participants were also the recipients of the passwords. They confirmed that they did not store the passwords after the tasks were completed. For instance, P20 did not store the password even though he could have if he wanted to:

Once a friend had a severe fever, and he could not withdraw cash on his own. He asked me to withdraw on his behalf and shared his card PIN. I had done such several times for others when they were incapacitated to transact on their own. They usually shared verbally, but I wrote them on a notepad and returned once the work was done. I did not keep any PINs out of courtesy. [P20]

Expectation of Reciprocal Password Sharing: When participants shared their passwords with someone, they also expected that the recipients would also share similar passwords with them. Such reciprocal expectations were mainly seen in romantic relationships – especially in unmarried relationships. Married couples also had mutual password share expectations; however, some non-tech-savvy wives

were also okay with letting their husbands manage their passwords without knowing their husbands' passwords. None of our participants who were having pre-marital romantic relationships mentioned accepting one-way password sharing. For instance, P3's (ex)boyfriend knew her social media passwords, but he did not share his password. P3 expressed her frustrations about such one-way password sharing, and she said she would demand her (to-be) husband's passwords before giving hers when the time will come. P12 expressed his reciprocal password sharing expectations with his (ex)girlfriend:

> *Its like...basically it was like...in this part of continent, trust is a big issue in relationship. What people think...what girls think is that my boyfriend is doing something bad – I need to know what he is doing (laughing). I heard that type of statements. So I felt like okay – if sharing password ensure peace, then be it. So I just gave. After giving the password, I felt like – okay, I gave her the password so now I need to know her password. So I took her password from "grudge" like I gave my password to her so why should not I know hers? [P12]*

Expectation of Surveillance: The expectation of surveillance played an essential role in password-sharing attitudes in Bangladesh. Surveillance was expected in both parental and romantic relationships. Parental surveillance was culturally expected and accepted by our participants. As a result, when participants shared their passwords of mobile phones with their parents for various reasons (e.g., making phone calls), they expected their parents to check their messages, photos, or other private data to find out about their romantic relationships.

In romantic relationships, passwords of mobile phones and social media were also shared. When the sharers shared the passwords of these devices and accounts, they expected that their partners might check their private activities. They still shared the passwords because it also meant that they had nothing to hide. Sometimes, people needed to change their behaviors expecting surveillance. For instance, P18 stopped flirting with other girls on Facebook because his girlfriend had his password and might see it. Password sharing was also considered an expression of "trust" – whether the partners trusted each other enough to be fully transparent.

Expectations of the Password-Recipients

Entitled to know the password: Sometimes the recipients of the passwords acted like they were entitled to know the passwords of the sharer. The sense of entitlement usually comes from the depth of relationships and password-sharing nature. First of all, the sense of entitlement was evident in parents-children relationships. Parents, especially mothers, thought they were entitled to know their children's phone passwords and could access them anytime they wanted. For instance, they could take the phone to call anytime. In some contexts, parents could also ask for passwords and perform surveillance as a part of parenting. P22 explained such a situation where her mother could ask to check her smartphones anytime:

> *It was 2010, and I was using a smartphone. My mom would check my Facebook, text messages, and messenger. [...] I was not allowed to have a password on my phone. My mom would be angry if I did. My mom was like, I need to give my phone access to my mom whenever she asks for it. She says that she needs to know what her daughter is doing. I have no issue with it. [P22]*

Sometimes, children also felt like they were also entitled to know their parents' passwords if needed. It was not like they could ask for it anytime without any necessity. However, they believed that they could have their parents' passwords anytime if needed for an emergency. For instance, P5 could access his mother's phone anytime if he needed to make calls cause he did not have a sufficient balance. P14 did not know his father's mobile banking password, but he believed that he could know it if needed:

> *I do not know his [father] password, but I know he has a bKash account, and I know the account number. I do not know the password. [...] He will definitely tell me the password if needed. It is just I do need that password, and that is why I do not know. When I need to do some transaction, he goes to the shop and does those by himself. [P14]*

Sometimes, in romantic relationships, people felt that they were entitled to know each other's passwords. Sometimes, it appeared like password sharing was a part of regular lives for such a sense of entitlement. For instance, it was common among couples (both marital and extra-marital) to share the banking card passwords and let the other use them for paying in restaurants or shopping malls, even in their presence. P9 mentioned how password sharing was integrated into his marital life:

> *We both log into each other's Facebook ID and roam around - sometimes for any family issues or sometimes without any reason we do so. I see her calling from my Facebook ID. Or, if I need to call her family, I use her Facebook to make the call. Or, if she talks to my family, she uses my Facebook. Like this. The same thing happens with WhatsApp. We see each other's wall and posts as well. [P9]*

Because of such a sense of entitlement to know the passwords, participants also felt like they were entitled to get explanations if such relationships stopped sharing passwords suddenly. In romantic relationships, if any partner stopped sharing passwords suddenly, it was perceived as hiding something from their partners. Questions like what they were hiding and what changed would usually come to the other partners' minds. Therefore, participants expected explanations, including the answers to those questions. P10 described his expectation for the explanation in case of terminating password sharing:

> *...[If I stop sharing my passwords with my wife] I would have to provide proper logic – why am I doing this now? If I had done it from day one – then it would have been normalized by now. [...] If I had any compromising situation; for instance, I faced problems (it can be financially as well) because of sharing passwords with her, then she would understand. Whereas, without proper reasoning, she would ask why have I been giving the passwords for years but what changed now. [I will also accept] if by sharing passwords with me, she faced some compromising situations. [...] It will be wrong if I say it [wanting to keep privacy] is not logical. However, I would still want to know why this sudden change of mind. [P10]*

Expectation of Transparency: In romantic relationships, the recipients of the passwords usually expected transparency from their partners. One of the ways to be transparent was to share social media passwords. Trust played an essential role in both marital and extra-marital relationships, and being transparent was sometimes one of the pre-requisites of earning trust. In other words, to achieve trust, partners needed to share their passwords to become transparent. P20 explained such a context:

> *When it is about a romantic relationship, I have seen people tend to share each other's passwords in this part of the world. They at times initiate the relationship based on the fact that they will be sharing their passwords. As if it is one's right to be able to observe the other's life on Facebook. Even my ex-girlfriend, right after we started dating, asked me if I could share my password. [P20]*

In romantic relationships, some participants described that they mutually felt they needed to know each other's passwords to be transparent. Also, sometimes, if one partner in the relationship demanded to know any password, then the other also wanted to have the same passwords to be transparent to each other. P4 described such mutual expectation of password sharing -

> *In a conversation in her [colleague's] presence, her colleague told me – Bhaia [Bangla word for calling elder brother], her (male) friend knows her password. Friend means her boyfriend. Furthermore, she also knows his Facebook password. They know each other's Facebook passwords because they are concerned about their partners chatting or how many male and female friends they have. They want to see these things. These types of practices are common in our society. [P4]*

Expectation to Assist: In our interviews, we noticed the dependency on children to operate and troubleshoot digital accounts. The parents of our participants were usually not that tech-savvy. They needed technical assistance to operate their mobile phones, manage social media accounts and digital financial accounts. The adult children usually took care of these technical problems of their parents, and part of the assistance required them to know the passwords if they did not already. Therefore, when participants received their parents' passwords, they generally expected to help them technically with the passwords. P19 described his obligation to help his parents technologically:

> *I live inside Dhaka, but it is not like they [parents] live far from Dhaka. The distance between my place and their place is around 15 kilometers. I usually visit them once a week. Sometimes they call me and let me know if they face any issues like something is not working. So when I visit them, I usually take care of their minor mobile issues and support them. [...] For instance, my mom says suddenly that she cannot connect her phone to the Wi-Fi. In that case, I reset the Wi-Fi password and log her in. Sometimes she does not get good internet speed. I check that on her phone why she is not getting that. Most of the cases, their complaints are like these – they are not getting internet speed, youtube is not working. [P19]*

Friends usually did not expect passwords of each other. They usually either asked for help or wanted to help. It was expected in friendships that friends would help each other. However, sometimes, the only way to help friends or get help was by password sharing. For instance, one of P4's friends was having a problem on his Facebook,

which he failed to fix. So P4 took his password and checked what was happening there to help him. In P4's words -

> *My other friend named X - a few years back, he called and told me that he installed an app and the app was posting some vulgar posts on Facebook. He had mobile access, but he was unable to grasp what was happening. So he gave me his Facebook credentials and told me to look at it using a web browser (I was in the office then). Then I saw he installed some apps, giving those full access. The apps were posting those junk posts. [P4]*

5.2 Cultural Factors of Password Sharing

Cultural beliefs and practices played an important role in password-sharing in Bangladesh. Gender, social norm, religion, and political context impacted what passwords, which whom, and when they needed to be shared.

5.2.1 Gendered Mothers' Role

Participants mentioned that children were obsessed with Youtube, and they usually used their parents' phones. However, children had more access to their mothers' phones than their fathers'. For instance, P5 mentioned that he knew the password and had access to his mother's phone to make calls anytime, but he did not have any access to his father's phone. Culturally, mothers' devices are considered as shared devices in the family. Besides, children were more comfortable taking mothers' phones because they were usually scared of taking their father's. P4, a father of two children, described the situation:

> *They [children] mostly use their mother's phone. They take my phone hardly and for a very short time to look at any photos or something. I do not give them my phone frequently because I have Gmail and bank account apps installed on my phone.[...] So Yes, we all have access to her mobile phone. It seems like we all use her phone. [P4]*

5.2.2 Gendered Password-Sharing Related Harassment

One of the biggest problems of password sharing was harassment. When participants talked about harassment, they mainly talked about how women's private information was leaked and used to harass them. It appeared like the women were more vulnerable than men by the same kind of harmful actions. Women usually faced harassment when their romantic relationship broke, and the ex-partner had access to their social media. Some boyfriends leaked personal photos, chats, and videos and sometimes impersonated the girlfriends on their social media to harass them. For instance, one of P18's male friends had access to his girlfriend's social media. He used to log into his girlfriend's account and abused her male friends from the friend list. P8 described the harassment that her female friend faced after her breakup -

> *I am not talking about myself – I am talking about my friend. She shared her Facebook account password with her boyfriend. That boy was a "bad guy." He found some personal information from her Facebook and later used those in a harmful way. I felt terrible – I think she should not have shared her password...He showed her private conversations to his friends. It is bad to show personal conversations with someone, right?... He showed those in personal chats, and he also uploaded the screenshots of the conversations in his Facebook story. [P8]*

Sometimes women had to leave social surroundings in some extreme cases if the leaked data was very sensitive and caused social reproach. P22's female friend had to leave school because one of her videos went viral –

> *When I was in class 9, one of my friends had an incident. Facebook was not there back then. There was one platform called hi5. I do not know much as I did not use the internet back then...So, some of her friends shared a sensitive video of my friend that went viral. My friend left the school for this. After this, I was very scared of the internet in general. [P22]*

On the contrary, harassing men in Bangladeshi culture was not that easy with similar actions. None of the participants mentioned any harassment that happened to men. P4 mentioned that his colleague's girlfriend removed some female contacts from his Facebook; however, he did not face any privacy leak and could mitigate the incident quickly. P12 did not even change his Facebook password after breaking up because he did not think that her girlfriend could harass him. In his own words:

> *Yes, I thought about it [harassment]. But again, I thought how much she could do there – she could knock my friends or posted something bad on my account. When something is done – it is done. I do not think we will do something like this – I have that strong belief. I do not know, but I do believe that. [P12]*

Women in Bangladeshi culture would hardly show such audacity with their accounts in the similar context.

5.2.3 Gendered Surveillance

Women's vulnerability in Bangladeshi culture impacted how their parents or elder siblings supervised their digital behaviors. Both male and female participants mentioned surveillance by parents and elder siblings, but the nature of surveillance was different based on gender. The parents and elder children usually do not monitor the younger male children's digital activities. Sometimes elder siblings remained vigilant so that the younger brothers did not get access to adult videos. However, the romantic relationship of the younger brothers was accepted and silently ignored by the elder brothers. P20 described his relationship with his younger brother:

> *I used to watch Japanese anime with some adult content that I did not want him [younger brother] to watch. I used to keep those files hidden. It was also when internet access was not widely available. So, we mostly watched movies on the phone. I kept other things hidden. But later, he grew up, and he watched similar stuff on his own. There has not been a need to hide things afterward [...] I have never monitored him intentionally, but I accidentally noticed a few of his activities. For instance, his phone rang, and the screen was lit with the picture of the person who called [younger brother's girlfriend]. I realized just looking at the phone who called and what the relationship was, that is it. I ignored it. [P20]*

On the other hand, both parents and elder siblings (usually elder brothers) monitored women to check they did not get into any romantic relationship. One of the reasons could be the existing vulnerability of women in Bangladeshi society, where it was easy to harm and harass women. For instance, even after completing her bachelor degree, P3 had to suffer strict surveillance where she had to share passwords of her mobile phone devices:

> *My family is a bit conservative, and I was never in such a relationship ever. During my Master's program, I met him and grew a relationship. During that*

> *time, my phone was seized or checked for messages by my family. My parents, especially my elder brother who is a defense official - his psychology is a bit different. So I would always keep my phone clean. I would delete the call history or chat afterward. [P3]*

5.2.4 Gendered Hierarchy of Technical Assistance

We noticed a gendered hierarchy of technical assistance in our interviews. Men were considered more technically sound than women; hence, men were the most preferred option for technical assistance. In marital relationships, husbands were found to create and manage their wives' passwords of different accounts. However, wives did not ever assist their husbands in this way. P6 described how he technically assisted his wife –

> *I think my wife belongs to analog time. I cannot say she belongs to digital time (laughing). She likes to use a button[feature] phone comparing to a smartphone. So, most of the time, I have to remember her passwords. I mean, I created most of her passwords. I did not write them down for her, but I told her the passwords verbally. I think she does not remember any of those. If I am not there, I do not think she can access the accounts. I believe she has forgotten all of her passwords. [P6]*

Our participants mentioned that their parents needed technical assistance to operate technology devices and digital websites. Parents usually chose elder children for such assistance. If the elder child was a daughter, they then took technical assistance from her in case there was no younger son. If there was a younger adult son in the household and no elder son, then the younger son handled the technical problems. P16 was the youngest son of the family, having three elder sisters. He mentioned assisting one of his elder sisters as well with her social media:

> *The problem was that – she [elder sister] already shared her password with "someone" you know. He logged into her account; therefore, my sister was not able to log in. My sister thought her account got hacked, so she shared her password with me to fix it. Then I accessed the account using the mail and password. Later we deactivated that account. [P16]*

Usually, if there was no elder brother in the family, the younger siblings took help opening accounts from the elder sister. For instance, P1 had a younger sister, and she

helped her open the Facebook account and managed her password. However, when P1 faced a problem with her social media account, she then took help from her cousin brother, who, she believed, was more technologically sound than she was.

Sometimes, some other credibility factors also played a role in changing the hierarchy of technical assistance. For instance, P21 was a banker, and her mother trusted her with her online banking credentials, including talking to customer care, although there was an elder son in the family. P21's professional credibility changed the hierarchical dimension.

5.2.5 Parental Surveillance is Accepted

Parental surveillance was expected and accepted in the culture. However, participants were not happy about such surveillance. For instance, they repeatedly referred to them as "brown" parents with a criticizing expression that they should be like this. But they complied with the demand for surveillance in anyways. P22 described the nature of the surveillance that she faced when she was a medical student -

> *I was not allowed to have a password on my phone. My mom would get angry if I did. My mom was like, I need to give my phone access to my mom whenever she asks for it. She said that she needed to know what her daughter was doing. I had no particular issue with it. So, when I was in the hostel [student dormitory], I would use a simple PIN to unlock my phone, but no app locks were there back then. In fact, few friends also knew my phone passcode, and they could see what was going on. But whenever I was at home, I would remove the password for my mom because she would often check my phone. And at night, I would have to leave my phone with my phone before I went to bed. [P22]*

Some participants did not use passwords in the family context because passwords meant there was something to hide. For instance, P2 did not put any password in her Facebook or Messenger because the lock would create questions like what she was hiding there. So, if she did not have any lock, it would mean that she had nothing to hide and would not create suspicion.

P3 had to go through extreme parental surveillance, and she expressed her frustrations during the interview -

> *This is different from the Western world. In the West, they do understand personal space. Our parents cannot think of yet that their children might have*

> *personal lives. They still think we are kids. I completed my study at Asian University for Women in Chittagong and stayed on the campus. I studied there for five years. After five years, when I came back home, they still treat me the same way they treated me five years ago. My family does not want to understand that I completed my bachelor's and master's, and currently, I am doing a job. I might have a personal life. I might need personal space. Although I am currently single now, it is not the right action to check my phone. [P3]*

5.2.6 Culturally Impolite to Say "No"

In general, participants found it difficult to say no to password sharing with friends and colleagues. It was culturally impolite to say no on the face when someone asks for something. Also, password sharing was a widespread scenario, and other people around them also shared passwords. Therefore, people might find it impolite if the participants had not shared their passwords when asked. For instance, P15 could not say no to her colleagues when they asked for her bank card pins for availing of a promotional offer. She was also okay with this sharing because she noticed her other colleagues doing the same. She feared rejecting request to share a password might harm the relationship. P9 also shared passwords because he did not want to be impolite, but he described his uncomfortable feeling during the interview –

> *At work – someone would say that their system was not working. Can I use yours? - They are colleagues, so I cannot say just no on the face. Although everyone signs that we will not share the passwords, but we all do it. So I cannot say no. Even though I feel uncomfortable, I would have to share the password. To be on the safe side, after they finish the task, I change the password. [P9]*

5.2.7 Impact of Religion in Password Sharing

Religion, especially Islam, also played an essential role in password sharing and password sharing-related issues. For instance, the family's religious background impacted the women's role and nature of surveillance. Participants, especially female participants, repeatedly mentioned that they came from "conservative Muslim" families to describe the nature of parental surveillance. Besides, religion also defined what data

was sensitive to them. For instance, the women who wore the hijab, they considered non-hijab portrait photos too sensitive to be seen by others or get leaked. This belief sometimes led them not to share the passwords or at least, become extra cautious when sharing was a necessity. For instance, P25 wore hijab, and head-covering was really important to her. When P25's phone was giving trouble, she was very concerned about her non-hijab photos as the technician who would repair the phone might see those. Therefore, she uploaded the photos on her Facebook with "only me" access and removed the photos from the phone. P25 also had to share her phone with relatives' children when they came to visit. She mentioned remaining vigilant while such sharing so that they could not go to her photo album where she kept her non-hijab photos. Similarly, P21's sister used App lock to protect her non-hijab photos -

> *I have seen my sister using an app lock to her gallery. She does so because she covers her head in public, and she does not want others to see any "uncovered" pictures unless it is one she wants them to see. I never really practiced it like that. [P21]*

5.2.8 Impact of Political Context in Password Sharing

The political context of Bangladesh also played a vital role in password sharing. Currently, Bangladesh is not in a state of assuring freedom of speech. According to Human Rights Watch 2021 report, "Bangladesh's Awami League-led government doubled down on an authoritarian crackdown on free speech, arresting critics, and censoring media. Arrests under the abusive Digital Security Act (DSA) increased dramatically" [35].

In such a political situation, participants mentioned their concerns about the security of their accounts. For instance, P14 was very concerned about his Facebook account and password because he saw in the news that provocative and anti-government speeches were spread from someone's account, but the account holder had no clue about that. Therefore, he never shared his account password with anyone fearing such harm. P6 was a social activist, and one of his friends was the victim of such a situation that P14 mentioned. P6 did not share passwords with his wife, but

he mentioned he was planning to share the password just as a precaution in such a political context. In his own words:

> *You know we do not have the right to free speech in our country. Someone can abduct me anytime because I am writing something against the ruling government. In that case, if someone close to me has access, they might give me some sort of support. At least they can stop the "illegal" access by the government. I am talking about the current context of our country. I know it from one of my very close acquaintances. He was abducted and locked up for eight days. He had two mobile phones, and they seized both of the phones. I have seen that now he is terrified of using a new mobile phone or laptop. He does not share anything on Facebook now that might cause him trouble. For instance, he does not say anything against the government. He gave all of the passwords to his wife to delete/deactivate the accounts if he gets abducted again. I think this will be a solution for the people like us who like to criticize and are advocates of free speech.[P6]*

5.3 Password-Sharing Model

Our password sharing model (Figure 5.2) describes the impact of cultural factors on different stages of password sharing. We identified three sequential stages of password sharing: motivation to share passwords, expectations for password sharing, and decision to share passwords. We also identified four cultural forces that affected *the identity* of the password sharer and the password recipients: gender roles, social norms, religion, and political context. These factors gave participants several identities like gender identity (man/woman), religious identity (Muslim/non-Muslim), cultural identity (collectivist/individualistic) and political identity. Participants' perceived identity dictates their motivation and expectation of sharing passwords – the stages that eventually form their decision to share passwords.

5.3.1 Cultural Forces and the Identity

From our initial axial coding, we identified four cultural forces that had an impact on password sharing. When we analyzed the data again closely along with the background information (Section 2.4), we identified that these forces did not impact password sharing directly; instead, they *created* the identity of our participants. In turn,

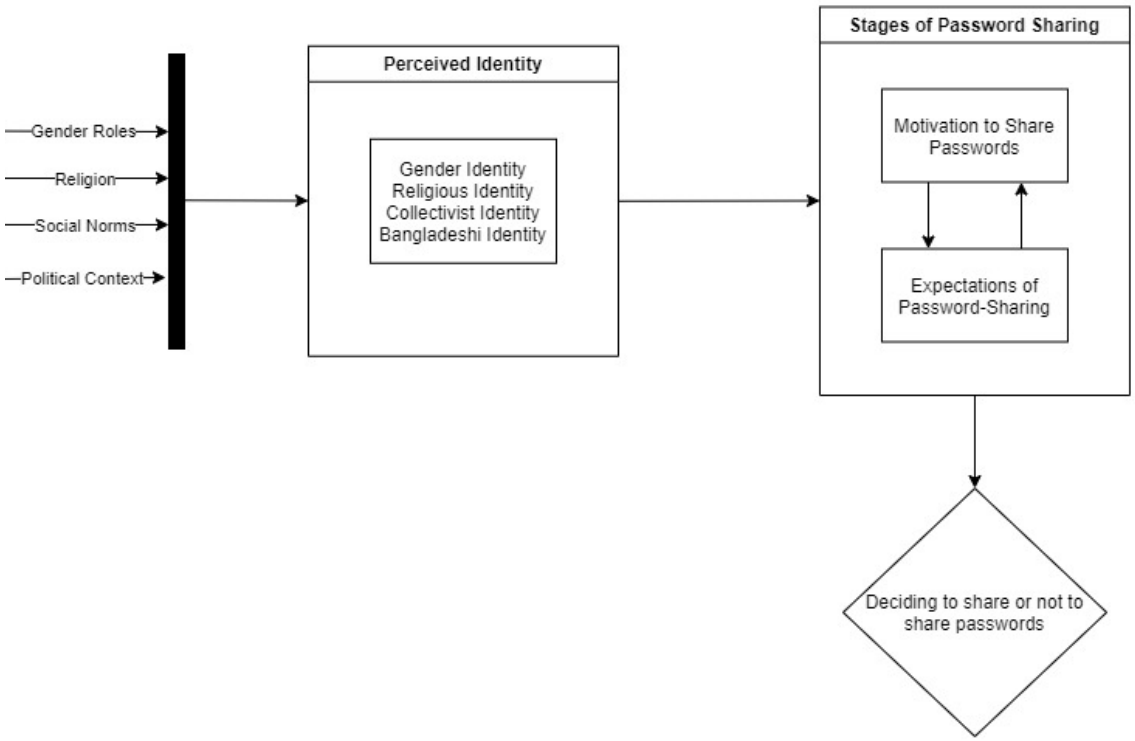

Figure 5.2: Diagram showing proposed relationships among cultural forces, perceived identity and the stages of password-sharing.

the participants' identity imposed some rules, beliefs, and expectations on other people's actions, which motivated them to share their passwords voluntarily.

Gender roles gave gender identity. Gender played an essential role in defining *identity*. Both men and women had different roles and expectations in society; therefore, motivation and expectations of password sharing also differed from gender to gender. For instance, it was socially expected that children and husbands would have access to mothers' phones. However, it was also socially accepted if the fathers did not give similar access to their children. So, usually women felt socially obliged to share their mobile devices with their children, whereas men did not.

Religion gave religious identity of Muslim/moderate Muslim/non-Muslim. In our interviews, participants described ways in which religion defines accepted and unacceptable actions from religious viewpoint, which also indirectly dictate what information will be private and not. Most of the Bangladeshi population follows Islam, and Islamic identity is sometimes more important for some people than other identities [33]. Such identity also shaped participants' motivation to share (or not share) passwords. For instance, the hijab was important to some of our Muslim female participants; therefore, they considered their "non-hijab" photos very private, and needing to be protected from surveillance. They usually did not share their phones to keep the photos out of signt. However, some other Muslim (and non-Muslim) women may not subscribe to the same definition of religious identity, meaning "non-hijab" photos might not have similar sensitivity.

Social norms gave collectivist identity. Social norms refer to social guidelines of acceptable and unacceptable behaviors or actions of the member of the society. These norms may be either unique to a specific culture or common in multiple cultures. Social norms also have an impact on participant's identities. For instance, one of the social norms of Bangladeshi culture is for people to help each other, often though by "sharing" (property, personal belongings like clothes, and technologies). According to Hofstede's definition, this cultural characteristic is called the collectivist dimension. In this way, social norms create the collectivist identity of Bangladeshi people. This identity motivates them to "help" because they are supposed to help

others, and the person receiving help is entitled to get the help. So when our participants shared their passwords, they were not only sharing their passwords, but were also *trusting the password recipients with their secrets* and *helping them.*

Similarly, *surveillance* was also expected and accepted in society for collectivist identity. In the social context of Bangladesh, we use *surveillance* beyond its widely accepted denotation of checking private information – it also meant "looking out for each other". For instance, when mothers were monitoring their children – they were not surveilling them to check what they are doing. Instead, the mothers were surveilling the children to look after them to not fall into any danger. On the other hand, the children also accepted such "motherly behaviours" because they believed their mothers were monitoring them because they care about them, and it was a way of looking after them. We also found in our analysis that it was socially unacceptable to say "no" to any request on the face because this would be interpreted as unwillingness to help or trust. Thus, social norms defined the collectivist identity, making "sharing" and "surveillance" acceptable behaviors in society. This collectivist identity based on societal norms also motivated participants to share their passwords.

Political context shaped Bangladeshi identity. Political context also defined participants' political identity. Bangladesh is going through political turmoil, and freedom of speech is not expected there. Mass governmental surveillance was also implemented. This political context also dictated some people's password sharing decisions. For instance, some participants valued their political identity of being a Bangladeshi, and to their definition, they should have had the freedom of speech everywhere. However, the current political context of Bangladesh would not approve of such identity and beliefs, but policies have been implemented to punish such actions [35]. As a result, to preserve the perceived political identity of being a Bangladeshi who should expect freedom of speech, some of our participants were motivated to share their social media passwords with trusted partners for extra safety and backup option. Sometimes, participants were also cautious about sharing their social media passwords because any anti-government speech shared from their accounts might cause them grave danger.

Summary. Our identified forces created a cumulative identity of our participants

that we call "perceived identity". Perceived identity is hierarchical, meaning one identity could be more important than another identity. For instance, to some people, their religious identity could be more important than their political identity. The identity dictated participants' motivations and expectations for password sharing. Additionally, the forces sometimes impact on each other to create the identity. For instance, gender roles worked as a force in our model, and religion also had gender-specific expectations and guidelines. Therefore, the motivations of a Muslim woman in Bangladesh might be somewhat different from that of a non-Muslim woman.

5.3.2 The Identity and Stages of Password-Sharing

In our model, "perceived identity" refers to the cumulative identity created by the cultural forces described in the previous sections. Our participants valued some identities over others, and those choices impacted password-sharing stages. For instance, it was expected in religion that Muslim women should wear a hijab. However, culturally Bengali women are not expected to wear a hijab as it is not the part of their cultural attire. We saw some of our participants prioritized their Muslim identity more than their cultural identity and practiced wearing a hijab. It was also culturally acceptable not to wear them. Hence, defined perceived identity is very complex, with significant personal agency. Overall, our participants were either men or women, from either Muslim or non-Muslim backgrounds. All of them were from a collectivist culture; however, Western individualistic education also made them aware of privacy. They belong to the same political context, but they had different views on politics. These identities affected the stages of password-sharing.

Motivation to Share Passwords: We have described our findings of participants' motivation for sharing their passwords in Section 5.1.1. We found factors like necessity, propinquity, trust, and collaboration motivated people to share their passwords. For instance, the social expectation of Bangladesh is that people should trust their family members. Passwords (secrets) should thus also be trusted with family members. Usually, family members did not ask for passwords unless necessary, but an unwillingness to share would mean a lack of trust in them. Such cultural meaning

of passwords in terms of trust motivated users to share passwords. Similarly, collectivist identity motivated participants to share important passwords with friends to help them in times of need, collaboration, or cost-sharing. Gender roles also motivated participants to share their passwords; for instance, women usually shared their passwords with their mothers because they understood that their mother was looking after them.

Expectations of Password-Sharing: Our analysis of participants' expectations while sharing passwords is described in Section 5.1.2. When participants considered sharing their passwords, they had some preconceived expectations from the recipients of the passwords. For instance, when participants trusted their friends and family members with their passwords, they expected that they would not cause harm and obey norms such as voluntarily forgetting the passwords. For instance, when participants shared their banking credentials with close friends, they expected that their close friends would not harm them by stealing money from their bank. Similarly, the recipients of the passwords with collectivist identity usually expected that they are entitled to be trusted with the passwords. Such expectations from the recipients' end also motivated participants to share their passwords.

Chapter 6

Issues Arising

In this chapter, we discuss the issues that arose from conflicts between motivation and expectation of sharing passwords. Our participants mentioned facing different challenges while dealing with password sharing. One of the major issues related to password sharing was the conflict between motivation and expectations when sharing passwords. This conflict affected relationships and systems which caused tensions in interpersonal relationships, privacy, usability and security. We describe the tensions resulting from interpersonal conflicts in Section 6.1. Section 6.2 describes privacy issues that people faced while sharing passwords. We also identified some system usability issues that caused password-sharing to be more problematic, which we discussed in Section 6.3. Lastly, we found some security issues that resulted from password-sharing. We describe these security issues in Section 6.4.

6.1 Interpersonal Difficulties

"Interpersonal difficulties" arose when the tensions between motivation and expectations affected relationships. Due to these difficulties, our participants experienced emotional burdens and loss of relationships.

6.1.1 Fear of being Judged

Our participants mentioned that they were motivated to share their passwords in some relationships, but they expected not to be judged for their activities on those platforms. In reality, participants sometimes feared judgment and sometimes got bullied for their actions. For instance, one of our participants (female, married, 30 years old) mentioned facing mild bullying by friends for her Netflix-watching habits.

> ...there was this movie [on Netflix] "365 days" which got very popular in

> Bangladesh, and I watched it. Then, one of my friends asked me why I watched it. Then I told her that I would also be able to see what you watch. But we can indeed see what others are watching. I feel a little discomfort when the fun gets a little out of control; otherwise, it is okay. They are my friends, that too from schooldays [P22]

Some of our participants shared their passwords with their romantic partners because they wanted to establish transparency in their relationships. However, they expected their partners not to go through their data fearing their partners might form a false judgement about the people they interacted with. For instance, P3's boyfriend had access to her social media though her phone. She mentioned that she was worried because her boyfriend might get hurt or judge her friends if he read the chat history. She used to delete the chats/messages with her friends before meeting her boyfriend.

Our participants obeyed parental control and surveillance, but they expected their parents not to use the access to ruin their relationships with friends. For instance, one of P22's male friends called her over the phone at 11 pm, and her mother received the call. Her mother regarded the friend as misbehaving because he was calling her daughter at late-night. But P22 was a first-year university student then, and the call was made to let her know about an exam the next day. She later forbade her male friends to call her over the phone and instructed them to send messages over Facebook, which her mother could not operate for the lack of technical competency.

6.1.2 Impersonation

Password sharers usually expected that the password recipients would not use the account access to impersonate them. However, participants mentioned that sometimes the recipients impersonated the account owners and interacted with their friends. For instance, P22 did not have a smartphone and accessed her Facebook using her roommate's mobile phone. P22 expected her roommate not to access the account, but she later found out that her roommate was chatting with her Facebook friends from her Facebook. As P22 described:

> *I logged in using her phone a couple of times, so she [roommate] had the password. She had misused this access. I came to know later. Friends would*

> *come to me and say about conversations I never had. It happened because she would communicate using my access and delete the conversation so that I do not have a clue. I got to know this within a month. So, I changed my password right away. [P22]*

Participants mentioned that children also sometimes accessed their parents' phones and posted on their behalf. P21 advised her colleagues to lock their WhatsApp and Viber apps so that their children could not accidentally send something to work related chat-groups. P4's children once took his phone to watch a video on Facebook, and he found them giving a "like" on that video after watching it. He then lectured them, saying that people might think he has given the "like"; therefore, they should not do such a thing while using his Facebook.

6.1.3 Changing Information

When participants shared their passwords, they expected that the recipients would not change anything without their approval. However, participants mentioned incidents where their information was changed using the access that they gave by sharing passwords. This type of behavior was noticed both in family relationships and in office life. These incidents caused hassles and sometimes put the account owners in awkward situations. For instance, P4 mentioned an incident where his colleague shared his Facebook password with his fiancé, and she deleted all his female friends from the friend list. She also mistakenly deleted some of his female relatives, including one of his maternal aunts. Sometimes, work passwords were shared for collaboration; however, uninformed information changes caused hassle in overall task completion. For instance, P7 worked in procurement and used an enterprise resource planning software (ERP) for work. She mentioned facing problems in the workplace because her supervisor sometimes changed information accessing her account without notifying her.

> *In between indent and purchase order issue – a change can happen in two sectors -purchase order issued or pending. So if you change something in between, the system will not notify you that something else has been modified. So I cannot verify if the price or condition has changed before issuing the purchase order. So if he [boss] changes anything there, it is really difficult for me to track back...I [once] faced the commercial team that the price has been changed. Then I had*

> *to sit with him again with the commercial. The changes are actually made for valid reasons – it is not like corruption or something like that. Since he does not inform me, I later face problems finishing the task. [P7]*

6.1.4 Harassment

Password sharing also sometimes led to harassment. When people shared their passwords with friends and boyfriends, the password recipients sometimes invaded the sharer's privacy and performed harmful tasks like blackmailing with private information, stalking, and showing personal information to others.

People usually shared their passwords in romantic relationships to prove that they did not have anything to hide and they were committed to the relationships. People also did not expect any harm in this kind of sharing. But relationships do not always work, and people end relationships. The end of relationships for women sometimes resulted in harassment from the boyfriends. For instance, some of our male participants mentioned having male friends who stalked their ex-girlfriends on Facebook using shared passwords. The victims of such harassment sometimes had to deactivate accounts. As P24 shared her friend's experience:

> *I had a friend who shared her phone, social media, and PC passwords with her boyfriend. And I think he had remote access. Later, when they broke up, he started to blackmail her. The boyfriend could see who is calling and whatnot. She had to stop using her phone, and she used mine for personal calls. The ex-boyfriend changed her Facebook password and started to post their pictures together. She suffered a lot. She had to deactivate that account then and had to reopen another account. [P24]*

6.1.5 Loss of Trust

The primary motivation for sharing passwords was to help in case of necessity. But sometimes our participants mentioned distrust caused by password-sharing which also ended relationships. When the password of an account was shared, and some harmful consequences happened, the victims might blame the person with whom they

had shared the password. In other words, the trust - which motivated such sharing, might be lost. For instance, P6 used one of his neighbor's laptops to purchase a train ticket. He also helped him opening his account there and buying a ticket. Later, both of their accounts were compromised, and some tickets were purchased using their cards. However, the neighbor eventually blamed P6 because he was a computer science student and thought he was involved in it. Although they could sort out the problem with the bank, the relationship did not work out. As P6 mentioned his feelings:

> *...So this was a bad incident. The worst part was that the brother thought I was the one doing it because I opened the account. Also, some transactions were made from my account using his credit card. That was a bitter experience, actually. [P6]*

6.2 Privacy Issues

Password sharing necessarily compromises the existence of privacy, meaning people give up some of their privacy when they share their passwords. However, even when people shared their passwords with someone, they expected the password recipient to respect their privacy by not sharing their information with others. This expectation was not always met, and we noticed password-sharing causing privacy issues.

6.2.1 Sharing Shared Accounts

Participants mentioned sharing subscription-based entertainment accounts with multiple people (usually friends) to divide the subscription fees. They typically used these shared accounts as if these were their private accounts and made privacy choices accordingly. Such behavior was widely seen when participants shared subscriptions of entertainment accounts like Netflix. Some of our participants mentioned sharing their Netflix accounts that had been shared with them by their other family members and friends. Most of the time, other sharers did not know about such sharing. Thus, the shared account was shared in another layer of relationships, and the viewing history became open to new layers. It was noticed that participants did not think about

their other friends' privacy when they shared their shared Netflix accounts with other friends and family.

6.2.2 Notification Privacy

Participants mentioned facing problems with notifications when they shared smartphones. They mentioned trusting that their device recipients would not snoop around to check personal chats or messages. However, notifications arriving while devices were shared resulted in recipients seeing messages unintentionally. P2 described such a situation:

> *I do not think they [younger siblings] check chats because they go through photos/videos or play some games. They use just for that purpose. So far, I know, they have never tried to check my Facebook messages or anything else. If they get some kind of notification, only then they got to know the message. Other than that, I do not think they pick on my accounts. [P2]*

Some participants mentioned their anxiety when they shared their phones with parents thinking friends or romantic partners might send texts, and the parents might notice that. P8 usually turned off his message notifications before sharing the smartphone with his parents.

6.3 Usability Issues

Passwords are designed to be individual, and there is often no option in the system for sharing them easily. As a result, participants faced different usability issues when passwords were shared with different relationships in different contexts. When people shared their passwords, they generally expected that the system would behave as if it accepted password sharing. In reality, the systems are often designed to prevent such sharing. The usability issues that came in our interviews are described in this section.

6.3.1 Multiple Access Problems

Our participants shared their passwords for helping in some relationships, but they never expected to lose access to the accounts. However, some systems did not accept

multiple concurrent logins from different devices, which caused participants to fear losing the account. For instance, P25 shared her bKash account with her friend, and later she could not access it and regretted the sharing. However, it was a multiple access problem, and she eventually figured that out. It was the security mechanism of the system that was causing the access issue. In P25's own words:

> *I gave my PIN [to a close friend]. But quickly after that, I realized that I could no longer log into my account. It kept showing error messages. It never happened with my bKash. Although I did not have much balance in my bKash, I was still worried. I called my friend, and she told me that she also could not take any money from the account. Later, we realized that it showed an error since the account was accessed from 2 separate devices. So, she got out I could log in again, and the account was recovered. So, even though I did not lose anything, it was still very much unpleasant for me. [P25]*

Sometimes participants shared their passwords for collaboration, but the multiple access policy hindered them from doing so. For instance, one of P18's friends shared his EA Origin account password so that they could play together. But he could only play when his friend was not online because it permitted only one access at a time.

6.3.2 Password Management

Participants mentioned facing password memorability problems because of password-sharing as they also had to remember the shared passwords. Sometimes, participants were responsible for creating and managing their parent's and spouses' passwords on top of their own passwords. None of our participants used dedicated password managers for managing passwords. As a result, participants mentioned forgetting the passwords that they used for their parents or spouses. P22 described a situation like this:

> *Yes, I opened their [parents] Facebook accounts on their phones, and they have been using the same phone. But I have forgotten that password. Neither do they know their passwords. So, if the phones are lost, there is a worry that they will not be able to access the same accounts anymore. [P22]*

According to our interview data, password sharing increased the burden of password change. Sometimes, our participants wanted to share some accounts for a short period. They also expected not to share other account accesses through their shared

password of an account. To meet these expectations, participants sometimes had to change their passwords frequently. For instance, participants changed their passwords when they wanted to stop sharing an account with anyone. In some worst cases, frequent password changes resulting in losing the accounts for good. For instance, P6 kept his scripts in emails and drives and shared the passwords with colleagues and directors. After each sharing, he changed the passwords because he did not want them to have continuous access to his works. He explained how he lost access to the accounts:

> *I do not have access to the Gmail or Yahoo accounts that I opened back then [in 2002]. It is because I changed the passwords very frequently and forgot them eventually. [...]I remember that we used to share the account. We would not keep any personal stuffs in that account. But now, we do not have access to those accounts. I remember two of the accounts that I could not access after forgetting the password. [P6]*

Some participants reused the shared passwords in essential accounts like email and banking; therefore, they had to change the reused accounts' passwords as well.

6.3.3 No Password Change after Sharing

Participants mentioned that password sharing was not always planned in advance; instead, it was sometimes casual. This sharing was deliberate and positively regarded: the sharers usually do not try to hide their passwords, and it is acceptable if the recipients see them. For instance, P7 wanted to see a photo on her younger sister's phone, and her sister unlocked the phone in front of her to show it. That was how she got to know her sister's phone password. However, people typically did not change the passwords after such sharing. For instance, P7's sister did not change her password after the task was done, and P7 still could access the phone. Some participants also did not change the passwords even after termination of a relationships or the end of necessity. Sometimes they did not stop sharing for future convenience. P24 mentioned such convenience at his workplace:

> *I needed some files from my office desktop, but I did not go to the office. I had to request a colleague to log into my PC and give me those files...I shared the password over the phone, and the password was not changed as we often would need such support. We all have access to a few PCs that belong to our unit because we require different stuff at different times. [P24]*

6.4 Security Problems

Password sharing poses multiple security challenges. Some of the security problems arose from the usability issues that passwords were not designed to be shared. In this section, we discuss the security challenges that appeared in our interviews.

6.4.1 Insecure Password Behaviors

Due to password sharing practices, people had to remember not only their own passwords but also needed to manage and memorize their shared passwords. Participants mentioned that they created and managed their parents', partner's, and office colleague's passwords. To do so, they usually followed various insecure password behaviors, including writing passwords down, reusing passwords, and creating insecure or algorithm-based passwords.

Insecure Password Storage: Participants mentioned that had trouble remembering the passwords of their parents and spouses. Therefore, they usually wrote them down in notebooks or recorded them in other insecure ways. Participants also had to communicate these created passwords to the account owners (typically parents and spouses). The owners of the passwords also wrote the passwords down.

> *I actually opened their [parents'] accounts. I definitely know their passwords then. And definitely, they did not change their passwords. But what happened is that I did not remember the passwords as well. I wrote them the passwords. I did not store the passwords or never tried to re-enter. I cannot remember what those passwords could be.[...] I did not write the passwords down but I told the passwords to my parents verbally. My parents wrote them down in a diary. [P15]*

P9 mentioned that his wife sometimes took photos of the passwords or wrote them in the notes of the phone. Some participants thought writing passwords in a notebook was safe because no one would find them. P4 mentioned that he needed to take care of his employers' passwords, including their personal ones. He found it hard to remember all the passwords and kept them in a password-protected excel file.

> *I manage those passwords in a protected excel file. There are quite a lot of passwords, and I might forget as well. I keep that file on my PC, and also I mail myself the same file for the backup. I have to update this regularly, and I follow the same procedure. [P4]*

Creating Insecure Passwords: Participants mentioned when they had to create passwords for other people to use, they usually created simple passwords for them so that they could remember their passwords. This kind of attitude was prevalent when participants assisted elderly people to set up their passwords. However, sometimes, it was still too hard for both the password creators and the password owners to remember the passwords. P1 created her parents' passwords and shared her experiences with them:

> *I wrote them [parent's passwords] down on paper. I myself cannot remember all of their passwords so I have to write them down. Though the passwords are not that much strong, they are easy passwords so that they [parents] can remember. But they sometimes forget their passwords; therefore, I have to write them down somewhere so that I can access to their accounts if they forget their passwords by any chance. [P1]*

Algorithmic Passwords: Some participants faced problems remembering the passwords, especially when they had to remember the shared passwords. To ease the remembering process, they mentioned creating different algorithms. For instance, P7 mentioned that their office culture was to know everyone's passwords. What they did was that their passwords were the combination of their official ID and some other algorithm that everyone knew. Their ID could be found at the desks. So everyone could access the desktops of each other without remembering the passwords. This was the way the system admin set the passwords and the instruction was to change the passwords immediately. However, no one changed the passwords for such sharing convenience.

Password Reuse: Participants also had different patterns for creating passwords and reusing them. When participants had to remember the shared passwords of their spouse, parents, and siblings along with their own, they often ended up using 3 or 4 passwords and reusing them across the accounts. Sometimes, participants ended up sharing the reused passwords which further weakened security. P4 faced such a problem but he understood the threat and mitigated it:

> *What happened was that, I reused my Gmail account password on my smart TV. So, when I shared my tv's password with my relative, I had to change all of my sensitive passwords as well. It is also because the password that I reused and shared, one could easily guess my other passwords as well. [P4]*

6.4.2 Other Account Access by Sharing Device Passwords

When participants shared their device passwords (e.g., mobile phone or laptop passwords), they did not just give them access to devices; they gave access to multiple accounts that were signed in on those devices. Participants mentioned that they found it convenient to log into apps like Facebook, Viber, etc., on their smartphones and to save passwords in the browser's password manager on their laptops and desktops. P25 explained the context of such sharing:

> *It is not like I have shared passwords, but you know all passwords are in my laptop. So, anyone using my laptop can access my Facebook or any other account. Besides, at times, my friends would ask for my phone to log into their own messenger. I do not necessarily log out of mine; they add their accounts and use it. [P25]*

Participants typically did not take any measures to protect these accounts other than giving devices to people they trust.

> *I am not giving it to everyone. I am giving it to my wife, and I trust her. I am giving it to my nieces. Apart from that, I will not give it to anyone. [P19]*

6.4.3 Password Reset by the Recipients

Some systems let users change their passwords without any further verification. However, it complicated password-sharing, providing complete control to the password recipients to reset the passwords without letting the owners know about it. As a result, the owners might lose the accounts for good. P23 experienced a similar incident. For instance, P23 shared a gaming account with one of his friends, and somehow, he did not continue playing. The friend thought P23 would not return to play; therefore, he continued to use the account after changing the password set by P23. Later, after three years, P23 wanted to log in to the account and failed. He faced some hassles to recover the account:

> *...At that point, I even forgot whom I gave it [a gaming account password] to as three years have passed by. So, I contacted the server authority. They asked me if I shared the password with anyone since the record showed a voluntary password change. I really had to think back and called many people to figure*

out who changed the password. There was not really a bad consequence as he gave the account back, but I had to waste about a week to get it.[P23]

6.4.4 Social Engineering Attacks

The password sharing attitudes of Bangladeshi people were also used to scam people into sharing their passwords. Bangladeshi people were very used to sharing their passwords that they sometimes become negligent to the threat of truly malicious requests. One of the common scamming approaches was to ask the passwords of financial accounts, pretending the call was made from financial institutions. P8 described such a scam that happened to her brother:

My brother has a bKash account. Someone called him and said they called from the bKash service center and asked so many questions. The person asked for his bKash PIN in between questions, and my brother also gave his PIN. After some time, he found that someone withdrew 2000 BDT from his account. [P8]

6.5 Summary

Our proposed model of password sharing incorporates cultural factors to understand how passwords are shared in Bangladesh. We found that some cultural identities like gender, religion, collectivism, and nationalism formed the perceived identity of the people that impacted the stages of password sharing. We identified two stages of password sharing: the motivation stage and the expectation stage. These two stages usually helped users to form the decision of password-sharing. The conflicts between motivation and expectations during password sharing caused tensions related to interpersonal relationships and privacy. We also found system usability and security issues usually stemmed from the fact that security systems do not acknowledge password-sharing.

It is evident from the above discussion that the motivations to share passwords and expectations for sharing them often contradict each other, which caused interpersonal difficulties and security challenges. People were typically motivated to share

passwords to help someone or to show that they trusted them. They also expected their password recipients not to harm them or judge their activities in the shared accounts. For instance, participants shared their Facebook passwords with romantic partners, but they did not expect them to post something without their consent. Sometimes, participants did not even change the passwords after the relationships ended, expecting no harm from their former friends or partners. In reality, the recipients often failed to act according to these expectations, which caused emotional burden and sometimes real danger to the password sharers. For instance, when exboyfriends blackmailed their former girlfriends for their shared accounts' data, the owners often had to deactivate their accounts to mitigate the situation. Participants also expected that the security systems would acknowledge password sharing – meaning they would still have some control of their accounts even after sharing passwords with the recipients. However, some systems failed to provide such an option that let any users to change passwords without further verification. As a result, both emotional and security issues arose when either or both password recipients and the systems did not act according to the expectations of the password owners.

Our model is a simplified interpretation for representing cultural factors in password-sharing. It does not consider the reality of complex relationships in human life. Examining the arising issues, we realized our model also does not consider emotions that also might have impact on password sharing and interpersonal problems related to them. However, we feel that our model does lend insights into understanding and potentially accommodating the issues arising because of password sharing in Bangladesh.

Chapter 7

Conclusions

The goal of this thesis was to investigate the cultural factors that affect password-sharing attitudes of Bangladeshi people, applying an Emics approach. This thesis investigated how password sharing takes place in Bangladesh by exploring questions such as who shared passwords, what type of passwords were shared, why people shared passwords etc. We followed an Emics approach to explore intrinsic cultural aspects related to password sharing. We found that password sharing is a common phenomenon in Bangladesh, and Bangladeshi people shared their passwords for different reasons with different relationships.

Our interviews revealed that all of our participants shared their passwords with family and non-family relationships. They shared different passwords, including financial account passwords, social media account passwords, and physical device (e.g., mobile phone) passwords. Passwords were mainly shared voluntarily but also out of obligation. Participants shared passwords either verbally or by writing them down. Password sharing could be either brief or for an indefinite timeline. Our participants mentioned feeling both positive and negative about password sharing, based on the context of sharing. Participants also mentioned following different techniques when they shared their passwords to protect their data from surveillance.

We were especially interested in understanding the cultural factors that affected password sharing in Bangladesh. We found four cultural aspects that impacted people's password sharing. Our identified factors are gender roles, social norms, religion, and political context. We also identified stages of password sharing, where the motivation to share passwords and expectations of the sharing played an essential role in deciding whether to share passwords.

We identified a password-sharing model based on interviews with the participants. This shows how our identified cultural factors impacted the password sharing stages.

Our analysis identified a core category that we named "perceived identity" of the password sharer or the recipients, which was the center of our model. Our identified cultural forces acted upon how our participants formed and perceived their identity *hierarchy*, meaning one identity could be more important than another. For instance, some participants prioritized their Muslim identity over their Bangladeshi identity. However, to some participants, their Bangladeshi identity was vital. The perceived identity of our participants made them a part of social groups, and there existed an underlying tendency to portray a positive image in front of the social groups. It also impacted their sense of right or wrong, beliefs, values, responsibilities, and obligations. Thus, the perceived identity of the participants mediated the password-sharing experience. For instance, if participants perceived themselves as collectivists, then they might be motivated to share their sensitive passwords with their friends because an essential aspect of their identity was to help and trust each other. Their expectation in this kind of sharing was that the recipients would not harm them by misusing the password. Combining all these aspects, participants decided whether they would share the password or not.

Finally, we discussed what happened if the password-sharing experiences failed to meet the expectations of the password sharers. We identified emotional burden, cognitive load, and loss of access as the major issues arising from unmet password-sharing expectations. Participants also faced usability issues for not having easy and secure password-sharing options in system designs. Unmet expectations of the password sharers and lack of usability of current systems also created some security problems that only added severity to the negative consequences of password sharing.

7.1 Contributions

This thesis contributes to the literature on usable security in the following ways:

- In our preliminary work, we present a framework named "Emics-Etics for Usable Security" to apply cultural factors in security systems. We also present a cross-cultural literature review using our framework to highlight the differences between Eastern and Western cultures regarding security beliefs, understanding, and practices. Our initial literature review finds significant cultural differences

in security attitudes, and we suggest that cultural factors (e.g., trust, family values, and social norms) must be considered while designing and developing security mechanisms.

- We applied our proposed Emics approach to understand how users from Bangladesh (an Eastern culture) shared their passwords. The lead researcher grew up in Bangladesh and only recently moved to Canada. Using her expertise in the Bangla language, we conducted most of our interviews in Bangla. We translated the interview data into English and transcribed them for analysis. We performed a qualitative analysis to give the overview of password sharing in Bangladesh.

- We used the Grounded Theory methodology to analyze our interview data and identify a password sharing model that considers the impact of cultural forces in password sharing. According to our model, gender roles, religious identity, social norm-based collectivist identity, and political identity from a hierarchical perceived identity impacts people's motivation and expectations of sharing passwords. Motivation for and expectations of password sharing influence the decision whether passwords will be shared or not. Sometimes the motivation and expectation are contradictory, which causes tensions that affect relationships and systems. We identified issues that arose from these tensions: interpersonal conflicts, privacy issues, usability issues, and security issues. Our password-sharing model suggests the importance of understanding cultural factors to address issues relating to password-sharing..

7.2 Limitations

Our research has several limitations. We conducted a pre-questionnaire survey before recruiting participants to manage the diversity of our sample population. Nevertheless, our research faced constraints on generality by only having participants aged 18 to 39 years. The study was conducted online due to COVID-19 restrictions. The lead researcher shared the recruitment posters in her network in Bangladesh, and we followed a snowballing method to recruit participants. As a result, our participants

typically mirror the lead researcher's network: typically young, educated, they lived in a metropolitan city, and were tech-savvy enough to use video conferencing tools. We missed the elderly population of Bangladesh because of the online method of conducting the study. Also, none of our participants were from rural Bangladesh – where, we assume, password sharing might be different from what we have reported. We had 11 female participants, but only one of them was married, and none had children. Although we found some insights about how mothers shared their passwords in the household from participants, our study lacks primary data from married women who also have children.

Our Grounded Theory analysis resulted in finding the impact of "perceived identity" in password-sharing attitudes. We acknowledge our limited background about identity theories, which is widely studied in sociology. Our definition of "perceived identity" is completely based on our interview data, which might differ from established definitions and theories of the terms.

7.3 Future Work

Our research suggests several future directions. We believe our model provides insights to help to understand cultural factors in password sharing. However, different identity theories from sociology and psychology could be studied and applied to improve our model in the future.

More research that could be done is to conduct more interviews in person with Bangladesh's older populations and rural populations. Our participants already mentioned their perceptions about how their parents use and thought of technologies. However, we did not have any participants to represent that particular age group. We did not have any data to understand how rural Bangladeshi people shared their passwords. Both the older and rural populations of Bangladesh might not feel comfortable and interested in participating in interviews online. Therefore, in-person interviews and participatory studies could be conducted to understand their password-sharing attitudes. It will be interesting to see if we could find additional factors to integrate into our model. In future, our model also could be used to compare password sharing in Eastern countries with Western countries to better explore the issues that arose in

our study.

Our study also indicated some problems related to password sharing. Password sharing is not a stand-alone phenomenon, but factors like culture and relationship complexities are significantly intertwined. In future works, technological solutions should acknowledge such factors to provide a better solution to this problem. One approach could be to improve access control mechanisms, to better acknowledge relationship complexities in different cultural settings. New technologies should be designed and developed to provide secure password sharing when it is evident password sharing cannot be avoided. In our work, the password is typically interpreted as "access", and when people share their passwords, they give access to their online lives. Alternative technologies to share access without sharing passwords could also be studied in future.

References

[1] Anne Adams and Martina Angela Sasse. Users are not the enemy. *Communications of the ACM*, 42(12):40–46, 1999.

[2] Syed Ishtiaque Ahmed, Md Romael Haque, Jay Chen, and Nicola Dell. Digital Privacy Challenges with Shared Mobile Phone Use in Bangladesh. *Proceedings of the ACM on Human-Computer Interaction*, 1(CSCW):1–20, 2017.

[3] Syed Ishtiaque Ahmed, Md Romael Haque, Irtaza Haider, Jay Chen, and Nicola Dell. "Everyone Has Some Personal Stuff" Designing to Support Digital Privacy with Shared Mobile Phone Use in Bangladesh. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, pages 1–13, 2019.

[4] Aniqa Alam, Robert Biddle, and Elizabeth Stobert. Emics and Etics of Usable Security: Culturally-Specific or Culturally-Universal? In *International Conference on Human-Computer Interaction*, pages 22–40. Springer, 2021.

[5] Deena Alghamdi, Ivan Flechais, and Marina Jirotka. Security Practices for Households Bank Customers in the Kingdom of Saudi Arabia. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, pages 297–308, 2015.

[6] Irwin Altman and Martin M Chemers. *Culture and environment*. Cambridge University Press (CUP) Archive, 1984.

[7] Robert Biddle, Sonia Chiasson, and Paul C Van Oorschot. Graphical passwords: Learning from the first twelve years. *ACM Computing Surveys (CSUR)*, 44(4):1–41, 2012.

[8] Franz Boas. *Race, language, and culture*. University of Chicago Press, 1982.

[9] Jan Lauren Boyles, Aaron Smith, and Mary Madden. Privacy and data management on mobile devices. *Pew Internet & American Life Project*, 4, 2012.

[10] Richard W Brislin. *Cross-cultural Encounters, Face-to-face Interaction: Face-to-face Interaction*. Pergamon Press, 1981.

[11] Richard W Brislin. Cross-cultural research in psychology. *Annual review of psychology*, 34(1):363–400, 1983.

[12] Peter J Buckley, Malcolm Chapman, Jeremy Clegg, and Hanna Gajewska-De Mattos. A linguistic and philosophical analysis of emic and etic and their use in international business research. *Management International Review*, 54(3):307–324, 2014.

[13] Afsan Chowdhury. Haunted by unification: A Bangladeshi view of partition. *Aljazeera*, 2017-08-15. https://www.aljazeera.com/features/2017/8/15/haunted-by-unification-a-bangladeshi-view-of-partition.

[14] Farah Deeba Chowdhury. Theorising patriarchy: the Bangladesh context. *Asian Journal of Social Science*, 37(4):599–622, 2009.

[15] Iftekhar Ahmed Chowdhury. *The Roots of Bangladeshi National Identity: Their Impact on State Behaviour*. Institute of South Asian Studies Singapore, 2008.

[16] Juliet Corbin and Anselm Strauss. *Basics of qualitative research: Techniques and procedures for developing grounded theory*. Sage publications, 2014.

[17] Raymundo Cornejo, Robin Brewer, Caroline Edasis, and Anne Marie Piper. Vulnerability, sharing, and privacy: Analyzing art therapy for older adults with dementia. In *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing*, pages 1572–1583, 2016.

[18] Paul Dourish. HCI and environmental sustainability: the politics of design and the design of politics. In *Proceedings of the 8th ACM conference on designing interactive systems*, pages 1–10, 2010.

[19] Paul Dourish and Ken Anderson. Collective information practice: Exploring privacy and security as social and cultural phenomena. *Human-Computer Interaction*, 21(3):319–342, 2006.

[20] Paul Dourish and Genevieve Bell. *Divining a digital future: Mess and mythology in ubiquitous computing*. MIT Press, 2011.

[21] Serge Egelman, Sakshi Jain, Rebecca S Portnoff, Kerwell Liao, Sunny Consolvo, and David Wagner. Are you ready to lock? In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, pages 750–761, 2014.

[22] Zillah R Eisenstein. *The radical future of liberal feminism*. Longman, 1981.

[23] Simson Garfinkel and Heather Richter Lipford. Usable security: History, themes, and challenges. *Synthesis Lectures on Information Security, Privacy, and Trust*, 5(2):1–124, 2014.

[24] Gerry Smith. Netflix, HBO and Cable Giants Are Coming for Password Cheats: Password resets and thumbprints are among the tactics being considered, 2019. https://www.bloomberg.com/news/articles/2019-11-08/netflix-hbo-and-cable-giants-are-coming-for-password-cheats, Last accessed on 2019-11-30.

[25] Google. Pixel phone help, 2020. https://support.google.com/pixelphone/answer/2865944, Last accessed on 2020-05-08.

[26] James E Gruber and Lars Bjorn. Women's responses to sexual harassment: An analysis of sociocultural, organizational, and personal resource models. *Social Science Quarterly*, 67(4):814, 1986.

[27] Alina Hang, Emanuel Von Zezschwitz, Alexander De Luca, and Heinrich Hussmann. Too much information! user attitudes towards smartphone sharing. In *Proceedings of the 7th Nordic Conference on Human-Computer Interaction: Making Sense Through Design*, pages 284–287, 2012.

[28] Marvin Harris. History and significance of the emic/etic distinction. *Annual review of anthropology*, 5(1):329–350, 1976.

[29] Geert Hofstede. National cultures in four dimensions: A research-based theory of cultural differences among nations. *International Studies of Management & Organization*, 13(1-2):46–74, 1983.

[30] Geert Hofstede. Dimensionalizing cultures: The Hofstede model in context. *Online readings in psychology and culture*, 2(1):8, 2011.

[31] Geert Hofstede, Gert Jan Hofstede, and Michael Minkov. *Cultures and organizations: Software of the mind*, volume 2. Mcgraw-hill New York, 2005.

[32] Hofstede Insights. Compare countries, 2020. https://www.hofstede-insights.com/product/compare-countries/, Last accessed on 2019-11-30.

[33] Akhand Akhtar Hossain. Islamic resurgence in Bangladesh's culture and politics: Origins, dynamics and implications. *Journal of Islamic Studies*, 23(2):165–198, 2012.

[34] Shahnajz Huda. Perspectives on Sexual Harassment in Bangladesh: Acknowledging its Existence. *Empowerment*, 6:22, 1999.

[35] Human Rights Watch. Bangladesh: Events of 2020. *Human Rights Watch*, 2020. https://www.hrw.org/world-report/2021/country-chapters/bangladesh.

[36] Anne Jonas and Jenna Burrell. Friction, snake oil, and weird countries: Cybersecurity systems could deepen global inequality through regional blocking. *Big Data & Society*, 6(1):2053951719835238, 2019.

[37] Michael L Jones. Hofstede - Culturally questionable? In *Oxford Business & Economics Conference*, Oxford, UK, 2007. Oxford Business & Economics Conference.

[38] Natasha Kabir. Cyber Crime a New Form of Violence Against Women: From the Case Study of Bangladesh. *Available at SSRN 3153467*, 2018.

[39] Jade Kake. *Rebuilding the Kāinga: Lessons from Te Ao Hurihuri.* Bridget Williams Books, 2019.

[40] Amy K Karlson, AJ Bernheim Brush, and Stuart Schechter. Can I borrow your phone? Understanding concerns when sharing mobile phones. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 1647–1650, 2009.

[41] Joseph 'Jofish' Kaye. Self-reported password sharing strategies. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 2619–2622. ACM, 2011.

[42] John N Kraay. Emics, Etics, and Meaning, an Exploration. *Philosophia Reformata*, 41(1-2):49–71, 1976.

[43] Alfred Louis Kroeber and Clyde Kluckhohn. *Culture: A critical review of concepts and definitions.* Peabody Museum of Archaeology & Ethnology, Harvard University, Cambridge, Massachusetts, USA, 1952.

[44] Michael Kwet. Digital colonialism: US empire and the new imperialism in the Global South. *Race & Class*, 60(4):3–26, 2019.

[45] Walter J Lonner. Issues in cross-cultural psychology. *Perspectives in cross-cultural psychology*, pages 17–45, 1979.

[46] Salvador Mandujano and Rogelio Soto. Deterring password sharing: User authentication via fuzzy c-means clustering applied to keystroke biometric data. In *Proceedings of the Fifth Mexican International Conference in Computer Science, 2004. ENC 2004.*, pages 181–187. IEEE, 2004.

[47] Tara Matthews, Kerwell Liao, Anna Turner, Marianne Berkovich, Robert Reeder, and Sunny Consolvo. "She'll just grab any device that's closer" A Study of Everyday Device & Account Sharing in Households. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, pages 5921–5932, 2016.

[48] Diana J Meter and Sheri Bauman. When sharing is a bad idea: the effects of online social network engagement and sharing passwords with friends on cyberbullying involvement. *Cyberpsychology, Behavior, and Social Networking*, 18(8):437–442, 2015.

[49] Shahrina Mou. Possibilities and Challenges of ICT Integration in the Bangladesh Education System. *Educational Technology*, 56(2):50–53, 2016.

[50] Laura L Murphy and Alexandra E Priebe. "My co-wife can borrow my mobile phone!" Gendered Geographies of Cell Phone Usage and Significance for Rural Kenyans. *Gender, Technology and Development*, 15(1):1–23, 2011.

[51] Fayika Farhat Nova, Md Rashidujjaman Rifat, Pratyasha Saha, Syed Ishtiaque Ahmed, and Shion Guha. Silenced Voices: Understanding Sexual Harassment on Anonymous Social Media Among Bangladeshi People. In *Companion of the 2018 ACM Conference on Computer Supported Cooperative Work and Social Computing*, pages 209–212, 2018.

[52] Borke Obada-Obieh, Yue Huang, and Konstantin Beznosov. The burden of ending online account sharing. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, pages 1–13, 2020.

[53] The Editors of Encyclopaedia Britannica. Nuclear family. *Encyclopedia Britannica*, 2015-11-1. `https://www.britannica.com/topic/nuclear-family`.

[54] The Editors of Encyclopaedia Britannica. Joint family. *Encyclopedia Britannica*, 2017-07-20. `https://www.britannica.com/topic/joint-family`.

[55] Kenneth L Pike. *Language in relation to a unified theory of the structure of human behavior*, volume 24 of *Janua Linguarum. Series Maior*. Walter de Gruyter GmbH & co KG, Berlin, Germany, 2015.

[56] Nimmi Rangaswamy and Supriya Singh. Personalizing the shared mobile phone. In *International Conference on Internationalization, Design and Global Development*, pages 395–403. Springer, 2009.

[57] Paul Ratazzi, Yousra Aafer, Amit Ahlawat, Hao Hao, Yifei Wang, and Wenliang Du. A systematic security evaluation of Android's multi-user framework. *arXiv preprint arXiv:1410.7752*, 2014.

[58] Marie Reay. *Being black: Aboriginal cultures in "settled" Australia*. Aboriginal Studies Press, 1988.

[59] Gordon Renouf. *Book Up: Some Consumer Problems*. Australian Securities and Investments Commission, Sydney, NSW, Australia, 2002.

[60] Nithya Sambasivan, Garen Checkley, Amna Batool, Nova Ahmed, David Nemer, Laura Sanely Gaytán-Lugo, Tara Matthews, Sunny Consolvo, and Elizabeth Churchill. "Privacy is not for me, it's for those rich women": Performative Privacy Practices on Mobile Phones by Women in South Asia. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*, pages 127–142, 2018.

[61] M Angela Sasse. Computer security: Anatomy of a usability disaster, and a plan for recovery. In *Proceedings of 2003 Workshop on Human-Computer Interaction and Security Systems at CHI*, 2003.

[62] Chara Scroope. Bangladeshi culture. *Cultural Atlas*, 2017. https://culturalatlas.sbs.com.au/bangladeshi-culture/bangladeshi-culture-references#bangladeshi-culture-references.

[63] Kate Senior, John Edward Bern, and David Perkins. *Variation in material wellbeing in a welfare based economy*. South East Arnhem Land Collaborative Research Project, University of Wollongong, Wollongong, NSW, Australia, 2002.

[64] Richard Shay, Saranga Komanduri, Patrick Gage Kelley, Pedro Giovanni Leon, Michelle L Mazurek, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. Encountering stronger password requirements: user attitudes and behaviors. In *Proceedings of the Sixth Symposium on Usable Privacy and Security*, pages 1–20, 2010.

[65] Ben Shneiderman and Catherine Plaisant. *Designing the user interface: strategies for effective human-computer interaction*. Pearson Education India, 2010.

[66] Barry Shore, AR Venkatachalam, Eleanne Solorzano, Janice M Burn, Syed Zahoor Hassan, and Lech J Janczewski. Softlifting and piracy: Behavior across cultures. *Technology in Society*, 23(4):563–581, 2001.

[67] Supriya Singh, Anuja Cabraal, Catherine Demosthenous, Gunela Astbrink, and Michele Furlong. Password sharing: implications for security design based on social practice. In *Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 895–904. ACM, 2007.

[68] Supriya Singh, Anuja Cabraal, Catherine Demosthenous, Gunela Astbrink, and Michele Furlong. Security design based on social and cultural practice: sharing of passwords. In *International Conference on Usability and Internationalization*, pages 476–485. Springer, 2007.

[69] Gayatri Chakravorty Spivak. *In other worlds: Essays in cultural politics*. Routledge, 2012.

[70] Steenson, Molly and Donner, Jonathan. Beyond the personal and private: Modes of mobile phone sharing in urban India. In Ling, Rich and Campbell, Scott W, editor, *The reconstruction of space and time: Mobile communication practices*, volume 1, pages 231–250. Transaction Publishers Piscataway, NJ, 2009.

[71] Elizabeth Stobert and Robert Biddle. Authentication in the home. In *Workshop on Home Usable Privacy and Security*, 2013.

[72] Taslim Taher and Mohd Adam Bin Suhaimi. Risks and harm on the internet among the teenagers in Bangladesh. In *2016 4th International Conference on Cyber and IT Service Management*, pages 1–4. IEEE, 2016.

[73] The Economist. As it turns 50, Bangladesh is doing well, despite its politicians. *The Economist*, 2021-03-27. https://www.economist.com/asia/2021/03/27/as-it-turns-50-bangladesh-is-doing-well-despite-its-politicians.

[74] The Economist. Bangladesh's growth has been remarkable, but is now at risk. *The Economist*, 2021-03-27. https://www.economist.com/leaders/2021/03/27/bangladeshs-growth-has-been-remarkable-but-is-now-at-risk.

[75] Hugh Russell Tinker. Bangladesh. *Encyclopedia Britannica*, 2021-03-10. https://www.britannica.com/place/Bangladesh.

[76] Harry C Triandis. Reflections on trends in cross-cultural research. *Journal of cross-cultural psychology*, 11(1):35–58, 1980.

[77] Nada Hamadeh Umar Sherajuddin. New World Bank country classifications by income level: 2020-2021. *World Bank Blogs*, 2020-07-01. https://blogs.worldbank.org/opendata/new-world-bank-country-classifications-income-level-2020-2021.

[78] Richard Vokes. Before the call: Mobile phones, exchange relations, and social change in south-western Uganda. *Ethnos*, 83(2):274–290, 2018.

[79] Alma Whitten and J Doug Tygar. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In *USENIX Security Symposium*, volume 348, pages 169–184, 1999.

Appendix A

Coding Process

A.1 Open Coding Table

We had in total of 168 open codes. In the table, four of our initial axial codes and associated open codes are given.

Category Name	Open Code	Description
Cultural Factors	Gendered Harassment of Password Sharing	Typically women faced harassment for sharing passwords.
	Gendered Hierarchy of Technical Assistance	Men were more preferred for technical assistance than women.
	Gendered Mothers' Role	Children typically used mother's phones comparing to their fathers'.
	Gendered Surveillance	Women were monitored to restrict having romantic relationships.
	Gendered Technical Competency	Men were more technically competent than women.
	Surveillance by Parents is Accepted	Parents could monitor both male & female adult children.
	Impolite to say No	People hesitated to say no to pw sharing.
	PW Share is a Norm	People practiced pw sharing like that is how it should be.
	PW Means Something to Hide	Having pw raised suspicion.
	Religious Factor	Religion shaped what was considered as private and sensitive.
	Political Factor	Lack of freedom of speech had an impact on pw share.
Motivation of PW Share	Trust	People shared pw with whom they trusted.
	Depth of Relationship	Level of relationship built trust to share PW.
	Propinquity	Living in close proximity led to trust someone with pws.
	Expression of Trust	Sharing pws with someone meant trusting them.
	Do not think PW is Important	To some people, some of their pws were not important.
	Less Sensitive Information	People shared pws thinking they had nothing important there.
	Necessity	It was sometimes needed to share passwords.
	Collaboration	People shared pws to work in a team.
	Permission to Use	Participant felt in control when the people asked for pws.
	Technical Assistance	People shared pws for taking technical assistance.
	Help People	People shared pws because they wanted to help.
	Convenience	People shared pws to delegate woorks to others.
	Shared Finance	People shared pws to share the finance in the same household.
	Shared Subscription Fees	People shared pws to share subscription fees.
Expectation of PW Share	Entitled to Know PW	People felt they should know pws of some relationships.
	Explanation of No PW Share	People expected explanation if partners did not share pws.
	Expectation of Surveillance	In some pw sharing, people expected to get monitored.
	Expectation of Transparency	Some relationships expected pw sharing for transparency.

Category Name	Open Code	Description
Expectation of PW Share (cont.)	Expectation to Technically Assist	Participants felt in need of knowing pws to technically assist.
	Mutual PW Sharing	Sharing pws created expectation to get/give similar pws.
	Voluntary Forget PW	Expectation that recipients of pw will not remember the pws.
	Voluntary No Access	Expectation that recipients will not access any private data.
	Voluntarily No Harm	Expectation that recipients will not misuse data.
Problems of PW Share	Burden of Stop Sharing PW	stop sharing required efforts.
	Emotional Burden	Participants faced judgemental comments.
	Loss of Relationships	Pw share sometimes caused loss of relationships.
	Accidental PW Share	Pws sometimes accidentally got shared by shoulder surfing and inattention.
	Change Information	The recipient changed information without informing the owners.
	Giving Other Access	Device sharing meant giving access to other apps like Facebook.
	Insecure PW Behaviour	Participants created easy and guessable pws and reused them.
	Insecure PW Share Method	Participants shared pws verbally and in written form insecurely.
	No PW Change after Sharing	People sometimes did not change their pws even after sharing.
	Account Overuse	Shared accounts were sometimes used like it were recipients' accounts.
	Harassment	People sometimes were harassed using the information from shared accounts.
	Private Information Leaked	Sometimes people got to know private information from pw sharing.
	Invading Privacy of Shared Account	Sometimes participants shared the pws of shared accounts.
	Accessibility Problem	Participants sometimes could not access their shared accounts.
	Burden of PW Change	Participants felt the burden of pw change for pw sharing.
	Problem with Notification	Public notification configuration caused privacy leak while device sharing.
	PW Memorability	Requirement for remembering shared pws made memorability problem harder.
	Hacking and Prank	Sometimes people got pranked because of pw sharing.
	Piracy	Participants practiced piracy by sharing pws.
	PW Share Business	Illegal business of sharing pws of entertainment accounts.
	Legal-Illegal Dilemma	Participants were not sure if pw sharing business was legal or illegal.
	Scamming	PW sharing attitude of Bangladeshi people was used to scam them into sharing their pws.

Appendix B

Ethics Application

Our submitted ethics protocol form is shared in section B.5.

B.1 Survey Consent Form

Project Title: Cultural Factors in Password Sharing: A Case Study of Bangladesh

Name and Contact Information of Researchers: Aniqa Binte Alam, School of Computer Science, Carleton University, Email: aniqabintealam@cmail.carleton.ca

Supervisor and Contact Information: Dr. Elizabeth Stobert, School of Computer Science, Carleton University. Email: elizabethstobert@cunet.carleton.ca

Project Sponsor and Funder The Natural Sciences and Engineering Research Council of Canada (NSERC) Discovery Grant 111747: Cognition-Informed Authentication

Carleton University Project Clearance Clearance : 114925
Date of Clearance: 17 February, 2021

Invitation
We are asking you to complete this pre-screening survey to determine your eligibility for the study. You must be at least eighteen years of age and must speak English or Bangla fluently. You must use technology devices, including computer/mobile phones, may use the internet and social media, and may have previous password sharing experiences. This survey is being conducted by Aniqa Binte Alam (Email: aniqabintealam@cmail.carleton.ca) of the Carleton University, Department of Computer Science, working under the supervision of Prof. Elizabeth Stobert (Email: elizabethstobert@cunet.carleton.ca).

Objectives and Summary:
Passwords are designed to be inherently private and confidential; therefore, password policies strictly forbid to share passwords with anyone. But previous studies have shown that passwords "need" to be shared to accommodate culture-specific practices in some eastern cultures. In this research project, we will try to understand the cultural sensitivity lying behind password sharing attitudes in Bangladesh.

The aim of this survey is to evaluate the eligibility to participate in our main research. Successful candidates will be invited to participate the main interview via email. We estimate that the survey will take about 5 minutes to complete.

If you decide to withdraw after you submit the survey, we will remove your responses from survey data if you notify the researcher within 2 days of submitting the survey. We will immediately delete the data of the survey participants who will not be invited to the interview.

We will analyze the pre-screening survey responses and invite suitable candidates for the final interview. The interview can be in Bangla or English. Participation in this study is voluntary, and you may skip any questions that you wish during the interview. All interviews will be audio-recorded. If you do not consent to being audio-recorded you will not be eligible for the study.

Risks and Benefits:
We do not anticipate any risks from taking the survey, nor do we anticipate that you will derive any benefit.

Compensation:
Your participation in this survey is voluntary, and you may choose not to take part, or not to answer any of the questions. You will not be compensated for filling out the pre-screening survey.

Confidentiality and Data Storage:
We will treat your personal information as confidential, although absolute privacy cannot be guaranteed. No information that discloses your identity will be released or published without your specific consent. Research records may be accessed by the Carleton University Research Ethics Board in order to ensure continuing ethics compliance. Your data will be stored and protected by Qualtrics (server is located in Toronto), but may be disclosed via a court order or data breach. The results of this study may be published, but the data will be presented so that it will not be possible to identify you. All research data will be kept in password-protected USB drive.

REB Review and Contact Information:
This research has been cleared by Carleton University Research Ethics Board-B (CUREB-B Clearance 114925). If you have any ethical concerns with the study, please contact the Carleton University Research Ethics Board by email at ethics@carleton.ca.

Implied consent:
By completing the online survey, you are agreeing to participate in the study.

Direct Consent:
I voluntarily agree to participate in this study.

- Yes
- No

B.2 Pre-Screening Survey Questionnaire

1. Language preference for the study:
    - Bangla
    - English
2. Name —
3. Email Address (Please provide a valid email address. We will send you an invitation and other materials to your given email address.) —
4. Age
    - 18-29
    - 30-39
    - 40-49
    - 50-59
    - 60-69
    - 70+
5. Nationality
    - Bangladeshi-living in Bangladesh
    - Bangladeshi-living abroad
        - How long have you been living abroad?
    - Others (please specify) —
6. Gender
    - Female
    - Male
    - Non-binary/other gender identity
    - Prefer not to answer

7. Occupation —
8. Education (highest education completed)
    - Secondary School certificate (S.S.C) / O-level exam
    - Higher Secondary School Certificate (H.S.C) / A-level exam
    - Diploma
    - Bachelor (honor's)
    - Master's
    - PhD
    - Others (please specify) —
9. What type of degree do you have? (based on the answer of 8)
    - Computer Science degree
    - Engineering degree (excluding computer science)
    - Medical degree
    - Commerce Degree
    - Core Science Degree (eg., mathematics, biology, physics etc.)
    - Social Science degree
    - Arts degree
    - Trade school
    - Others (please specify) —
10. What devices do you use regularly? (choose all that apply)
    - Computer (Pc/laptop)
    - Feature phone (not smart phone)
    - Smart Phone
    - Tablet
    - Home IoT devices (e.g., smart assistant, hubs, smart tv etc.)
    - None
    - Others (please specify) —
11. What type of password accounts do you have? (choose all that apply)
    - Digital media accounts (Netflix, Googleplay, Spotify, Amazon , HBO, Youtube, Robi Tv+, Hoichoi, Binge. Bongo. Bioscope etc.)
    - Physical items (phone/tab/computer/smart hub, Wifi etc. password)

- Social media accounts (Facebook, Twitter, snapchat, instagram etc.)
- Online Banking accounts and card PIN (Online and mobile baking, Card PIN etc.)
- Online shopping accounts (Amazon, Daraz, Rokomari, Pikaboo etc.)
- Online household billing accounts
- Ride sharing applications (Uber, pathao etc)
- Dating applications (Tinder)
- Video conferencing accounts (zoom, google hangout, slack etc.)

12. Have you ever shared your password/someone's password?

    - Yes
    - No

13. Audio recording is mandatory for our study. Do you agree to be audio-recorded?

    - Yes
    - No

B.3 Interview Consent Form

Project Title Cultural Factors in Password Sharing: A Case Study of Bangladesh

Name and Contact Information of Researchers: Aniqa Binte Alam, School of Computer Science, Carleton University, Email: aniqabintealam@cmail.carleton.ca

Supervisor and Contact Information: Dr. Elizabeth Stobert, School of Computer Science, Carleton University. Email: elizabethstobert@cunet.carleton.ca

Project Sponsor and Funder The Natural Sciences and Engineering Research Council of Canada (NSERC) Discovery Grant 111747: Cognition-Informed Authentication

Carleton University Project Clearance Clearance : 114925
Date of Clearance: 17 February, 2021

Invitation
You are invited to take part in this research project because you are a Bangladeshi, must speak English or Bangla fluently, and be at least 18 years old with sufficient experience with technology devices. The information in this form is intended to help you understand what we are asking of you so that you can decide whether you agree to participate in this study. Your participation in this study is voluntary, and a decision not to participate will not be used against you in any way. As you read this

form, and decide whether to participate, please ask all the questions you might have, take whatever time you need, and consult with others as you wish.

What is the purpose of the study?
Passwords are designed to be inherently private and confidential; therefore, password policies strictly forbid to share passwords with anyone. But previous studies have shown that passwords "need" to be shared to accommodate culture-specific practices in some eastern cultures. In this research project, we will try to understand the cultural sensitivity lying behind password sharing attitudes in Bangladesh.

What will I be asked to do?
If you agree to take part in the study, we will ask you to attend an one hour long interview on Zoom where you be asked about your password sharing behaviours. It is important that you are alone while giving the interview in order to preserve the privacy of the interview. This is to mention that, we will not ask your passwords at any stages of our study. The interview can be in Bangla or English according to your preference. Participation in this study is voluntary, and you may skip any questions that you wish during the interview. All interviews will be audio-recorded. If you do not consent to being audio-recorded you will not be eligible for the study.

We will need your banking/bKash account information for e-transferring the compensation amount.

Risks and Inconveniences
We do not anticipate any risks to participating in this study. Considering the social and gender norms in Bangladesh, you might feel insecure when discussing some issues related to password sharing. You will not be asked to share your real passwords at any stages of our study. Please keep in mind that the research is voluntary and the interview is confidential, and will be coded to keep your identity obscure.

Possible Benefits
You may not receive any direct benefit from your participation in this study. However, your participation may allow researchers to better understand culture specific password sharing practices to address them in security tools design.

Compensation and Incentives
BDT 1000 compensation will be provided for participating in the interview. The compensation will be sent (e-transferred) to your bank account/mobile banking account (bKash). You may withdraw from this study at any time up to the end of the interview session. If you do choose to withdraw, you will still be compensated, and all data will be deleted from the study.

No waiver of your rights

By signing this form, you are not waiving any rights or releasing the researchers from any liability.

Withdrawing from the study
If you withdraw your consent during the course of the interview session, all information collected from you before your withdrawal will be discarded.

Confidentiality
We will remove all identifying information (e.g., name, email address etc.) from the study data as soon as possible, which will be seven days after the interview is conducted.

We will treat your personal information as confidential, although absolute privacy cannot be guaranteed. No information that discloses your identity will be released or published without your specific consent. Research records may be accessed by the Carleton University Research Ethics Board (CUREB B) in order to ensure continuing ethics compliance.

All data will be kept confidential, unless release is required by law (e.g. child abuse, harm to self or others).

The results of this study may be published or presented at an academic conference or meeting, but the data will be presented so that it will not be possible to identify any participants.

We will keep a master file with your name, account information and compensation confirmation receipt for the audit purpose. The master file will be kept in a password protected USB device which will only be accessible by the researchers.

You will be assigned a code so that your identity will not be directly associated with the interview/survey data you have provided. All study data, including coded information, will be kept in a password protected file on a secure computer.

Audio recording of your interview will be stored locally on the researcher's computer. Operation data, such as meeting and performance data, will be stored and protected by Zoom on servers located in the U.S.A, but may be disclosed via a court order or data breach. We will password protect any research data that we store or transfer.

Data Retention
After the study is completed, your de-identified data will be retained for future research use. We will keep the transcribed file but destroy the audio recording after one month of the study. All the data will be stored on password protected USB key.

Ethics review
This research has been cleared by Carleton University Research Ethics Board-B (CUREB-B Clearance 114925). If you have any ethical concerns with the study, please contact Carleton University Research Ethics Board by email at ethics@carleton.ca.

Statement of consent
I voluntarily agree to participate in this study.

- Yes
- No

I agree to be audio recorded during the interview.

- Yes
- No

(Note: audio recording is mandatory)

Signature of participant —
Date —

Research team member who interacted with the participant
I have explained the study to the participant and answered any and all of their questions. The participant appeared to understand and agree. I provided a copy of the consent form to the participant for their reference.

Signature of researcher —
Date —

B.4 Interview Guide

Hello, my name is Aniqa Binte Alam and I am a Master's student in the School of Computer Science at Carleton University. I am working under the supervision of Prof. Elizabeth Stobert.

I would like to invite you to participate in a study titled Cultural factors in Password Sharing: A Case Study of Bangladesh. This study aims to increase passwords' usability and minimize security threats caused by password sharing by incorporating relevant culture-specific practices in authentication design. We will not ask you to share your passwords at any stage of our studies.The study is funded by the Natural Sciences and Engineering Research Council of Canada (NSERC).

The study involves an interview where will ask questions regarding your understanding, beliefs and practices related to password sharing. All interviews will be audio-recorded. If you do not consent to being audio-recorded you will not be eligible for the study.

We estimate that the interview will take about 60 minutes to complete. Participation in this study is voluntary, and you may skip any questions that you wish during the interview. You may withdraw from this study at any time up to the end of the interview session. If you do choose to withdraw, you will still be compensated, and all interview/survey data will be deleted from the study.

BDT 1000 compensation will be provided for participating in the interview. The compensation will be sent (e-transferred) to your bank account/mobile banking account. The withdrawal will not have any impact on the compensation. You will not be compensated for filling out the pre-screening survey.

This research has been cleared by Carleton University Research Ethics Board-B (CUREB-B Clearance 114925).

If you are ready, please let us know and we will start the audio-recording.

Tentative interview questions

1. Do you have any [Category will come from the survey answers e.g., netflix/googleplay etc.] accounts that you commonly use? Choose all accounts from the following list. Based on the category,
    - With whom do you share this password?
    - Why do you share the password?
    - How do you share password?
2. Do you need to hide any account from anyone from your family?
    - Why do you hide it?
    - How do you hide it?
3. Do you use other people's account?
    - Why and how do you use it?
    - Which tasks do you usually complete?
    - What worked well and what didn't previously? (note: the researcher will follow up on these based on the participant's responses)

4. Do you feel that you are obliged to share your passwords?
    - When and by whom?
    - Which account is that?
    - Why do you feel the necessity?
    - What do you do about that?
    - Without sharing password, what you could have done in the same scenario?
5. Do you feel uncomfortable sharing your password?
    - Why do you feel uncomfortable?
    - Which account and with whom?
    - What do you do about it?
6. Have you ever faced any bad consequences for sharing password? Would you share the experience with us?
    - When, which account?
    - Do you still share passwords? Why and why not?
    - Do you now do anything different because of this?
7. Tell us if you stopped sharing any accounts with anyone and why?
8. Do you think password sharing is bad?
    - Why do you think that?
9. Do you have any Biometric passwords? (e.g., fingerprints, facial recognition, voice recognition etc.)
    - What type of Biometric password do you have? For which account?
    - Do you share them?
    - How do you share them?
10. Do you have any token based passwords? (e.g., card, password generator etc.)
    - What type of token based password do you have? For which account?
    - Do you share them?
    - How do you share them?
11. Do you have any two factor authentication?
    - For which account do you use 2FA authentication?

- What are these two types of authentication? (e.g., text based OTP, combination of password and finger-print etc.)
- Do you share them?
- How do you share them?

12. Do you think of any suggestion for current password sharing process?

Thank you so much for your responses. Since we are still looking for participants, please feel free to share the pre-screening survey link with your network.

Should you have any ethical concerns with the study, please contact the REB Chair, Carleton University Research Ethics Board-B by email: ethics@carleton.ca.

I am sharing debriefing materials with you via email. Please feel free to ask any questions related to this this study and I will be happy to answer. I am sending you the compensation using the information you provided via email.

If you have any questions about the research after this interview, please contact me at aniqa.bintealam@carleton.ca.

B.5 Ethics Protocol Form and other Supporting Materials

Our study received ethical clearance from the Carleton University Research Ethics Board B (clearance number 114925). Our submitted ethics protocol form is shared in the next page. We have also included supporting materials like email invitations, recruitment posters and debriefing materials in both English and Bangla languages that we submitted along with our ethics applications.

Office of Research Ethics
CARLETON UNIVERSITY

Research Ethics Protocol Form

This is the primary CUREB study submission form, to be used when none of the other submission forms, intended for more specialized categories of research, are suitable. If you have any doubt about which form to use, or for help in completing this form, please contact the Office of Research Ethics at ethics@carleton.ca or by phone: 613 520 2600 ext. 2517 (CUREB A) or ext. 4085 (CUREB B).

* Please submit this form as a new application in CuResearch. If this form is to replace a Release of Funds, it should be submitted as an "Event" in CuResearch under the same study file. Please see our CuResearch User Manual for directions on how to submit a new application or an event.

* Note that all of our forms are compatible with Microsoft Office. Students and staff members can download a free copy of MS Office at no charge: Students: https://carleton.ca/its/ms-offer-students/ ; Staff/Faculty: https://carleton.ca/its/all-services/computers/site-licensed-software/ms-offer-faculty/

1. Title and Date

1A Project Title

Title of Research Project (Detailed instructions, Example)

Cultural Factors in Password Sharing: A Case Study of Bangladesh

1B Submission Date

Date of completion of this form. Update each time the form is revised. (Detailed instructions, Example)

4 February, 2021

1C Attachments

List documents included with this application (e.g. consent materials, invitations, permissions) (Detailed instructions, Example)

Appendix 1: Supervisor Signature Form
Appendix 2: TCPS2 Certificates of the researchers
Appendix 3: Survey Consent
Appendix 4: Interview Consent
Appendix 5: Letter of Invitation to Organizations
Appendix 6: Email Invitation for Interview
Appendix 7: Recruitment Poster
Appendix 8: Online Invitation
Appendix 9: Email Invitation
Appendix 10: Debriefing
Appendix 11: Pre-Screening Survey Questionnaire
Appendix 12: Interview Guide
Appendix 13: Email for Ineligible participants
Appendix 14: Survey Consent – Bangla
Appendix 15: Interview Consent – Bangla
Appendix 16: Letter of Invitation to Organizations – Bangla
Appendix 17: Email Invitation for Interview – Bangla
Appendix 18: Recruitment Poster – Bangla
Appendix 19: Online Invitaton – Bangla
Appendix 20: Email Invitation - Bangla
Appendix 21: Email for Ineligible Participants - Bangla

2. Project Team

2A Lead Researcher

☐	Academic or Library Staff
☐	Post-doctoral Fellow
☒	Graduate Student
☐	Undergraduate
☐	Other

Last name/First name

Alam, Aniqa, Master's Candidate

Official university (or other institution) email address

aniqa.bintealam@carleton.ca

Department, faculty and institution (Detailed instructions, Example)

School of Computer Science, Faculty of Science, Carleton University

2B Academic Supervisor

☐	Same as lead researcher

Academic supervisor(s) Last name/First name. (Note, the supervisor must be copied on all correspondence with CUREB.)

Stobert, Elizabeth, Research Supervisor, Assistant Professor

Official university (or other institution) email address:

elizabeth.stobert@carleton.ca

Department, faculty and institution (Detailed instructions, Example)

School of Computer Science, Faculty of Science, Carleton University

2C Project Team Members

☒	No other team members

List the project team members: 1) Last name/First name 2) Email address 3) Role in project 4) Department and institution (Detailed instructions, Example)

3. Study Overview

3A Study Goal

What research question(s) will this study seek to answer (1-2 sentences)? (Detailed instructions, Example)

Passwords are designed to be inherently private and confidential; therefore, password policies strictly forbid sharing passwords with anyone. However, previous studies have shown that passwords "need" to be shared to accommodate culture-specific practices in some eastern cultures. This research project will understand the cultural sensitivity lying behind password sharing attitudes in Bangladesh. Bangladesh is an eastern country known for its collectivist culture where "sharing" is common in different life spheres. This study aims to identify and apply culture-specific practices related to password sharing in authentication design. We expect that our study will make the authentication systems more acceptable and usable to Bangladeshi users.

3B Study Purpose and Benefits

Study rationale: why should the research be pursued; what are the benefits, and to whom? (Benefits can be to research community, companies, or society in general.) (Detailed instructions, Example)

The design of authentication systems (such as, passwords) is euro-centric and tends to ignore the culture-specific practices of eastern users. Sharing attitudes are such cultural practice that are

ignored in authentication design. As a result, sharing passwords is not permitted by authentication design and policy. However, people from eastern cultures still share their passwords to comply with their cultural practices. They usually share their passwords for banking, social media, and entertainment accounts following unsecured procedures: writing them down on paper, sending them through SMS, email, and social media. These unsecured practices often result in credential fraud, account compromise, monetary loss, and cyberbullying.

In this project, we will study such culture-specific password sharing practices in Bangladesh so that we can address them in authentication design. It is one of the first studies investigating password sharing practices in Bangladesh. We will design a usable and secure mechanism to share passwords to make authentication design culturally appropriate and acceptable to the users from Bangladesh and similar collectivist cultures. Our study outcome will also increase overall computer security and create further research prospects.

3C Participant Interactions Overview

Briefly describe what will happen to, or will be required of, the participants during the research. (Only a project overview is required). (Detailed instructions, Example)

- Participants will be invited to participate through the letter, email, poster, and online invitation (See attachments: Letter of Invitation-Appendix#5, Recruitment Poster-Appendix#7, Online Invitation-Appendix#8, and Email Invitation-Appendix#9).

- Participants will be asked to fill out pre-screening survey questions so that we can evaluate their eligibility for the study (See attachments: Survey Consent-Appendix#3, and Survey Questionnaire-Appendix#11)

- Eligible participants will get email invitations for participating in the interview. The email will contain consent instructions (See attachment: Email Invitation for Interview-Appendix#6, and Interview Consent-Appendix#4). They will be instructed on how to sign the consent form digitally. An interview will be scheduled after receiving the signed consent form.

- During the interview, the participant will be introduced to the study's purpose. They will be reminded that the study is audio recorded. After getting permission from the participant, the researcher will start the audio-recording and commence the interview following the interview guide (See attachment: Interview Guide-Appendix#12). We will not ask the participants to share their passwords at any stage of our studies. We will investigate if they share passwords with anyone and their understanding related to this practices.

- The researcher will end the interview restating the data protection guideline and participant's rights towards the data (see attachment: Interview Guide-Appendix#12). They will be provided debriefing document (See attachment: Debriefing-Appendix#10) after the interview session and any questions of the participants related to the study will be answered. The participants will be

compensated afterward using their preferred methods. The study with the participant will end with this process.

3D **Minimal Risk Review Request**

☐	Yes, minimal risk review
☒	No, not minimal risk

Should this protocol be considered for minimal risk review? If so, please briefly justify. If not requesting a minimal risk review, leave this section blank. (CUREB will decide whether an application is reviewed at full board or via a delegated process). (Detailed instructions, Example)

3E **Dates of Recruitment/Participant Interaction**

Estimated date when will you will start recruiting participants? (YYYY-MM-DD)

2021-02-10

Estimated date when you will end participant interactions? (YYYY-MM-DD) (Detailed instructions, Example)

2021-12-30

3F **Additional Reviews**

☒	No additional review
☐	Departmental review
☐	Grant council review

Has this project been reviewed for academic merit? (not required, but for the Board's information) By whom? (e.g. a Tri-Council grant application or student's thesis committee) (Detailed instructions, Example)

4. Methods: Participants

4A **Description of Participants**

Describe the participants and any inclusion and exclusion criteria. If using a separate sample of control participants, describe this group. (Detailed instructions, Example)

We will recruit 50 study participants from Bangladesh who are at least eighteen years of age and must speak English or Bangla fluently. Participants must use technology devices, including computer/mobile phones, may use the internet and social media, and may have previous password sharing experiences. The participants matching the descriptions mentioned above will be asked to fill out a short online survey to determine eligibility. We are looking for participants from diverse background in terms of gender, age, education and occupation. We will analyze the survey responses and invite suitable candidates for the final interview. The individuals from Bangladesh who are not at least eighteen years of age and do not use any technology devices will be excluded from the study.

4B **Number of Participants (Sample size)**

How many participants will be recruited? If multiple groups of participants are involved, breakdown by participant type. Provide a justification including a statistical rationale if appropriate. (Detailed instructions, Example)

50 participants will be interviewed. It is expected that the study will reach theoretical saturation after this number of participants have been interviewed.

4C Vulnerable Population

☒	Not Vulnerable Population

Describe any vulnerabilities of the participant group(s) that may compromise their ability to give free and informed consent or cause additional risks. Describe your mitigation strategy to ensure valid consent. (Detailed instructions, Example)

Participants are not considered vulnerable.

4D Participant Relationship to Researcher

☒	No previous relationship
☐	Instructor-Student
☐	Client
☐	Employee
☒	Friends/Family
☐	Participated in previous study
☐	Other

Describe any relationship that exists between the participants and the research team or any recruiting party or sponsor. Indicate how relationships will be managed so there is no undue pressure on participants. (Detailed instructions, Example)

Recruitment materials will be distributed to the lead researcher's previous university and workplaces in Bangladesh. Therefore, there is a possibility that the participants may end up being known to the researcher as alumni or ex-colleagues. In such a case, the researcher will emphasize that participation is entirely voluntary and that participants may withdraw at any time. Participation will not affect personal relationships in any way.

4E Benefits to Participants

☒	No Direct Benefits

Describe any potential direct benefits to the research participants as opposed to society or knowledge. (Detailed instructions, Example)

There are no direct material benefits to study participants.

4F Benefits to Participant Community

☒	No Direct Benefits

Describe any benefits to your research participant community (e.g. indigenous community), such as capacity building, knowledge sharing, and fulfillment of community research priorities. (Detailed instructions, Example)

This research does not specifically involve indigenous participants.

4G Conflict of Interest

☒	No conflicts
☐	Financial benefit to researcher
☐	Benefit to Corporation
☐	Other

Describe any conflicts of interest, and indicate how they will be managed. (Detailed instructions, Example)

No conflicts.

4H Researcher Training with Participant Group

☒	Not applicable

In addition to the TCPS2 training, describe any additional training the researcher(s) have (or will receive) to work with the proposed participants (e.g. research with Indigenous communities). (Detailed instructions, Example, TCPS2 Training)

Researcher has no specific training.

5. Indigenous Peoples and Community Engagement

Research involving Indigenous/Aboriginal peoples

5A If none of the statements are applicable, skip this section (Detailed instructions, Example)

☐	Recruitment criteria includes Indigenous identity as a significant factor
☐	Study will seek input from participants regarding Indigenous communities, cultures, artifacts, traditional knowledge or unique characteristics
☐	Indigenous identity or membership in an Indigenous community is a factor in data analysis (e.g. sub-group analysis)
☐	Interpretation of the research findings will refer to Indigenous communities, peoples, languages, histories or cultures

5B **Consultation**

Describe the consultation process with the indigenous community/ies. What is the community's involvement in governance of the research? With whom did you consult and what arrangements, if any, were made to implement Tri-Council (TCPS 2 Chapter 9) principles? If no consultation has taken place, please explain. (Detailed instructions, Example)

5C **Approvals/Agreements**

As part of the above process, describe what approvals/agreements you have made with the participating community/ies. (Detailed instructions, Example)

5D **Benefits to Participant Community**

Describe how the research will provide fair benefits to the participating community/ies, meet community research priorities, support capacity building through enhancement of the skills of community personnel, and recognize the role of elders and other knowledge holders. (Detailed instructions, Example)

5E **Participant involvement in research findings**

Describe how participants will be given the opportunity to participate in the interpretation of the data and review of research findings prior to the completion of any reports or publications? If such participation will not occur, explain. (Detailed instructions, Example)

5F **Data Ownership, Control. Access and Possession**

Describe arrangements for the participating community's/ies' ownership and/or sharing of project data and findings, including the OCAP principles (ownership, control, access and possession).

6. Methods: Recruitment

6A **Recruitment Methods**

☐	Not applicable
☒	Posters
☒	Social Media

Describe each step of how participants will be recruited. This includes how prospective participants will be identified, how contact information will be obtained, how participants will be made aware of the study, and how participants can express their interest. Provide a copy of all the recruitment material(s) including any oral scripts, recruitment posters, recruitment emails, social media

☐	Online Panels (e.g. Qualtrics)
☐	Student Participant Pool (e.g. SONA)
☒	Emails
☒	Letters
☐	Telephone
☒	Snowballing
☐	Other

postings etc. (Detailed instructions, Example)

Step 1: The lead researcher is from Bangladesh, and she has existing connections with her previous university and workplaces. Besides, she has Bangladeshi friends on her social media. The lead researcher will make use of these connections for recruiting participants. The researcher will also ask the interview participants and Facebook friends to tell their friends, family, and colleagues about the study. The media and processes are described below in details:

- *Letter: the researcher will send the letter of invitation, poster, and the pre-screening online survey link to the Asian University for Women in Bangladesh (lead researcher's undergraduate university) and SSL Wireless Limited (a software company, lead researcher's previous workplace in Bangladesh) for distribution within their mailing list and notice board (See attachments: Letter of Invitation-Appendix#4, Email Invitation-Appendix#9, Recruitment Poster-Appendix#7, and Pre-screening Survey Questionnaire-Appendix#11). REB clearance is not required because they will be only putting up the recruitment posters/letters but we will be conducting the recruitment ourselves.*
- *Social Media: the researcher will advertise the recruitment notice, including the pre-screening survey link on Facebook among her connections (See attachment: Online Invitation-Appendix#8, and Pre-screening Survey Questionnaire-Appendix#11).*
- *Snowballing will be used. Participants may share the Facebook notice and tell others about the study, who may likewise be interested in participating (See attachment: Online Invitation-Appendix#8, and Interview Guide-Appendix#12).*

Step 2: The participants will express their interest in participating by filling out the pre-screening survey. They will need to read and give online consent before starting the survey (See attachment: Survey Consent-Appendix#3, Pre-Screening Survey Questionnaire-Appendix#11).

Step 3: The researcher will analyze the survey data and select participants based on the information provided. Eligible participants will be invited via email (See attachment: Email Invitation for interview-Appendix#6). Non-eligible participants will be sent an email confirming they will not take part in the interview session (See attachment: Email for Non-Eligible Participants-Appendix#13).

6B **Location of Recruitment**

☐	Not applicable
☐	Carleton
☐	Other Canadian School/University

List all recruitment locations. If some locations require permission prior to recruitment, indicate if permission has been secured. (Detailed instructions, Example)

Recruitment will occur online.

☐	Canada
☒	Online
☐	Other

6C **Third Parties in Recruitment**

☒	Not applicable

If using third parties to recruit, indicate who is doing the recruitment and how it will be accomplished. Does the third party have the prospective participant contact information? Are community leaders involved in identifying potential participants? (Detailed instructions, Example)

N/A

6D **Recruitment risks to Participants**

☒	No risks

Describe any risks to participants during the recruitment phase, including risks to privacy. (Detailed instructions, Example)

We anticipate no risk to the participants during the recruitment phase. We will take the name and email address in the pre-screening survey, which will be stored and protected by Qualtrics, which has servers located in Toronto. We will analyze the survey data storing them in a password-protected USB drive. The ineligible participants' information will be deleted immediately after the analysis from both the Qualtrics server and USB drive.

6E **Recruitment risks to Researcher**

☒	No risks

Describe any risks to the research team during the recruitment phase. (Detailed instructions, Example)

None.

6F **Compensation**

☐	No Compensation
☒	Money / Gift Card
☐	Reimbursement of Travel Expenses
☐	Refreshments
☐	Course Credit
☐	Other

Describe all participant compensation and remuneration (including its monetary value) and indicate when participants will receive the compensation. What happens to the compensation if a participant withdraws? (Detailed instructions, Example)

Participants will be given 1000 BDT (Approximately 15.48 CAD). They may withdraw from this study at any time up to the end of the interview session. If they do choose to withdraw, they will still be compensated, and all study data will be deleted from the study.

The compensation will be sent (e-transferred) to the participants' bank accounts/mobile banking accounts (bKash). A For bank to bank money transfer, we would need to know participants' bank account number, bank account name, bank name and bank branch name. For a bKash transfer, we need to know bKash account phone number and account name. We will ask participants to share these information via email.

We will maintain a master file with user's name, account number and the confirmation email of the money receipt. The master file will be stored in a password-protected USB, which will only be accessible by the researchers.

7. Methods: Informed Consent

7A **Obtaining informed consent**

☒	Signed consent
☒	Online consent
☐	Oral consent
☐	Implied consent
☐	Parent/Guardian consent
☐	Assent
☐	Other

Describe the process for obtaining informed consent from the participants (or guardians/legal representatives). If written consent is not used, explain the alternative method chosen. Include a copy of all consent forms, scripts and other materials. (Detailed instructions, Example)

Participants will have to provide their consent for both the pre-screening survey and online interview. The invitation and consent form will be translated to Bangla and available to participants in language of choice.

For the online pre-screening survey, the participants will read the consent form and mark the box "Yes" for the statement "I voluntarily agree to participate in this study" to start the survey (See attachment: Survey Consent-Appendix#3).

For the interview, the researcher will send a consent form to the participants' email addresses. The participants will be instructed to read the materials and sign the consent form digitally. They will be reminded that the audio-recording is mandatory. If the participant agrees to participate, they need to mark "yes" to both "I agree to participate" and "I agree to be audio recorded" statements and sign the form digitally (See attachments: Interview Consent-Appendix#4, Email Invitation for Interview-Appendix#6). Participants will be ineligible if they do not want to be audio-recorded.

7B **Deception**

☒	Full Disclosure (i.e. no deception)
☐	Partial Disclosure
☐	Mild Deception
☐	More than Mild Deception

Describe and justify any deception and/or partial disclosure (e.g. what information is withheld). Describe the magnitude and likelihood of harm due to deception. Describe any planned secondary consent and include forms or text. (Detailed instructions, Example)

N/A

7C **Debriefing**

☐	Not required

Describe if, when, and how participants will be debriefed. (Include a copy of any documents that will be provided to participants). Describe any risks during debriefing and how they will be mitigated. (Detailed instructions, Example)

Participants will receive a debriefing document (See attachment: Debriefing-Appendix#10) at the end of the interview session. The researcher will provide answers to the participants' questions and ask them to reach out if they want to ask anything later (See attachment: Interview Guide-Appendix#10).

7D **Withdrawal Procedures**

☐	Not applicable
☒	Participants can withdraw
☐	Participants can only withdraw during the study session

Describe the procedures for a participant to withdraw. What will happen to data from participants who withdraw? Describe any deadlines and limitations on withdrawal, during the study or after research participation is complete. Explain if compensation amount is affected by withdrawal. (Detailed instructions, Example)

Participants may withdraw from this study at any time up to the end of the interview session. If they choose to withdraw during the interview session, they will still be compensated, and all study data

☐	Special withdrawal procedures	*will be deleted from the Qualtrics server and the researcher's USB. The data related to compensation (e.g., name, account number, and transaction confrmation emails) will not be deleted and stored in a password-protected USB file for audit purpose.*
☐	Full compensation to withdrawn participants	

8. Methods: Data Collection

8A **Data Collection Methods**

Describe in detail the method of data collection being used and provide details of any instruments used. Breakdown by phases, participant groups, or types if required. Complete the section on "online data collection" if relevant. (Fully describe or include a copy of any questionnaires, surveys, interview guides, or other data collection instruments). (Detailed instructions, Example)

☒	Questionnaires / Surveys
☒	Interviews
☐	Focus Groups
☐	Oral and/or Visual Stimuli
☐	Equipment and/or software testing
☐	Other

The study will take place online. It is divided into two parts: a) Online Pre-Screening Survey and b) Online Interview Session.

a) Online Pre-Screening Survey: The participants will be asked to fill out a short online pre-screening survey where they will be asked to provide consent to participate, their language preference, names, email addresses, demographic information, and password sharing attitudes (See attachment: Survey Consent-Appendix#3, and Pre-Screening Survey Questionnaire-Appendix#11). The survey data will be stored and protected by Qualtrics, which has servers located in Toronto. The researcher will download and save the data in a password protected USB for the analysis. The data of the non-eligible participants will be deleted immediately from the USB drive and Qualtrics server.

b) Online Interview Session: The successful candidates will be contacted via emails. They will be asked to sign the consent form and schedule the online interview using calendly.com (See attachment: Email Invitation for Interview-Appendix#6, and Interview Consent-Appendix#4). We will run a semi-structured interview (See attachment: Interview Guide-Appendix#12). The interview will take place on Zoom, and the entire session will be audio-recorded. The audio-recording of the interview will be stored locally in a password protected USB drive. Operation data, such as meeting and performance data, will be stored and protected by Zoom on servers located in the U.S.A.

Any data may become disclosed via a court order or data breach. We will password-protect any research data that we store or transfer. We will not ask the participants to share their passwords at any stage of our studies. We will investigate if they share passwords with anyone and their understanding related to this attitude.

8B **Location of Participant Interactions**

Where will the research procedures involving participants take place? (Detailed instructions, Example)

☐	Carleton
☐	Workplace
☐	Public venue

The research will take place online. The pre-screening survey will be conducted using Qualtrics, which has a reputation for providing customer data protection and reliability. All the communications with the participants will be conducted using the email platform.

☒	Online
☐	Outside Canada
☐	Other

We will schedule the meeting using the Calendly platform. The interview will take place on Zoom, and we will audio record the session. The audio recorded file and any research materials will be stored locally in a password protected USB drive. We will not ask the participants to share their passwords at any stage of our studies. We will investigate if they share passwords with anyone and their understanding related to this attitude.

8C **Frequency and Duration of Participant Interactions**

How many times will you interact with participants? How long will each interaction take? (Detailed instructions, Example)

The researcher will interact with the participant twice: a) Online Pre-Screening Survey and b) Online Interview. The online survey will take a maximum of 5 minutes to complete. The interview will take an hour to be completed. We will also communicate with the participants using email to invite them to the interview, send consent link and debriefing materials, and schedule the interview.

8D **Photography or Recordings**

☐	Not applicable
☐	Photographs
☒	Audio Recording
☐	Video Recording
☐	Other (Please describe)

If the participant will be photographed, video-recorded or audio-recorded, indicate how the data will be acquired and protected. How will consent for recordings be obtained? If other (e.g. fingerprints or eye-tracking) please describe. Can participants opt out of recordings and still participate? (Detailed instructions, Example)

In the interview session, the participants will be audio recorded using Zoom. We will take signed consent before the interview (See attachment: Interview Consent-Appendix#4). The participants will also be reminded that the session will be audio-recorded before turning on the recorder (See attachment: Interview Guide-Appendix#12). The participant cannot participate if they opt out of the recording.

8E **Translation or Transcription**

☐	Not applicable
☐	Translation
☐	Transcription
☒	Researcher will translate or transcribe

If you require the services of a translator or transcriber, describe what services you will use and how you will interact with the translator and/or transcriber. If a confidentiality agreement will be used, include a copy. (Detailed instructions, Example)

The Interview will be conducted in Bangla or English. The lead researcher is from Bangladesh, and Bangla is her first language. She will transcribe the audio recording into English.

The audio recordings of the interviews will be saved in a password-protected USB key. The researcher will transcribe it into English and save the transcribed file in the USB drive. The audio recording will be deleted from the USB key when data has been verified (e.g., comparing the audio data and transcriptions) and deidentified.

8F **Online data collection**

☐	Not applicable
☐	Carleton-based server
☒	Commercial server (based in Canada)

Describe the software platform used for online data collection, and the security of data storage. Where will data be stored? Will participant IP addresses be recorded? Are there any special limitations on privacy? (Detailed instructions, Example)

We will use both Qualtrics and Zoom platforms for data collection.

☒	Commercial server (outside Canada)
☐	Other

The pre-screening online survey data will be stored on a secure website, Qualtrics. Qualtrics employs multiple layers of security to make sure that data remains private and secure. All surveys created are placed in a Secure Survey Environment (SSE). The web pages are encrypted with a secure socket layer (SSL). Only persons with authorized access to a survey account can download the data from this server. Qualtrics is SAS 70 certified and meets the rigorous privacy standards imposed on health care records by the Health Insurance Portability and Accountability Act (HIPAA). All Qualtrics accounts are protected by password-access. Qualtrics employees will not access the protected accounts without express permission by the account owner. The Qualtrics Canada's data center is located in Toronto. Researchers will disable the option in Qualtrics to collect IP addresses.

Our interview will take place on Zoom, and the entire session will be audio-recorded. We will create separate meeting IDs for each interview session and it will be accessible by unique passwords. The audio recording of the interview will be stored locally in a password protected USB drive. Operation data, such as meeting and performance data, will be stored and protected by Zoom on servers located in the U.S.A. No audio-recording will be stored in the cloud.

We will not ask the participants to share their passwords at any stage of our studies. We will investigate if participants share passwords with anyone and their understanding related to this attitude. Any data may become disclosed via a court order or data breach.

8G **Biological specimens or fluids**

☒ Not applicable

Describe the apparatus and methods to collect biological specimens or fluids (e.g., blood, saliva, tissue samples). How will specimens be stored? If any will be retained or transferred to another institution/research group, explain the research purpose, and plans for eventual destruction, if any. (Detailed instructions, Example)

N/A

8H **Biological or physical interventions**

☒ Not applicable

Describe any drugs, devices or diagnostic apparatus being studied or used, or any physical or physically intrusive research interventions, such as sending energy into the body (e.g. electrodes, MRI/X-ray), or physiological activities (e.g. exercise or stress). Explain any risks to the participants and compare the dose to established safety standards. (Detailed instructions, Example)

N/A

8I **Risk of Psychological Harm**

☒ No risks

Explain the nature, magnitude and probability of these risks and how they will be mitigated. (Detailed instructions, Example)

N/A

8J **Risk of Physical Harm**

☒ No risks

Explain the nature, magnitude and probability of these risks and how they will be mitigated. (Detailed instructions, Example)

N/A

8K **Risk of Social and/or Economic Harm**

Explain the nature, magnitude and probability of these risks and how they will be mitigated. (Detailed instructions, Example)

☐	No risks

Mild (privacy issues) – considering the social and gender norms in Bangladesh, some participants might feel intimidated or perhaps insecure when discussing their feelings about password sharing. Participants will be reminded that there are no right or wrong answers to the questions asked of them. Furthermore, the research is voluntary, confidential, and will not result in any adverse consequences, including social and personal relationships. We anticipate no risk if a family member finds out that the individual is participating in the study. Participants will not know ahead of time what kinds of questions are being asked but they will know that the study is about password sharing. Also, we will not ask the participants to share their passwords at any stage of our studies.

8L **Incidental Findings**

Describe possible incidental findings and how they will be managed (e.g. becoming aware of abuse of a child, imminent harm to a participant or third party, or potentially significant clinical findings). Any resulting limitations of confidentiality should be communicated to participants. (Detailed instructions, Example)

☒	Incidental findings unlikely

The research team does not anticipate any incidental findings.

9. Methods: Data Storage and Analysis

9A **Identifiability of collected data**

Describe the identifiability of research data at the point of data collection. If there are different levels of anonymity for different groups, describe. (Detailed instructions, Example)

☒	Identifiable
☐	Coded (pseudonyms)
☐	Anonymous
☐	Other

The identifying information (e.g., pseudonym, phone number, Zoom ID, email address) of the successful participants will be saved on a password protected USB key, which will be stored in a locker in the PI's home.

9B **Identifiability of stored data**

Describe the identifiability of stored research data. If a link to participant identities is retained (e.g. to permit compensation or withdrawal), also explain storage of linking data. Describe the process of anonymization if applicable. (Detailed instructions, Example)

☐	Identifiable
☒	Coded (pseudonyms)
☐	Anonymous/anonymized
☐	Other

After data collection, each participant will be given a code name, and the transcripts will be labeled with this code name. Interview transcripts will be altered to remove all real names and identifying information (e.g., where they work). Once interview data are transcribed, verified (e.g., comparison between the audio-recorded interviews and transcriptions have been made), and de-identified, the audio data will be destroyed.

9C **Identifiability of published data**

Describe the identifiability of data that will appear in publications, including how pseudonyms will be assigned, if applicable. If there are different levels of anonymity for different groups, describe each

☐	Anonymous

☐	Aggregate data only
☒	Pseudonyms/Coded
☐	Real participant names with data attributable
☐	Other

level here. (Detailed instructions, Example)

Responses will be non-attributable. Participants will be assigned a code name during analysis.

9D **Data Storage (during the project)**

☐	Encrypted
☒	Password-protected
☐	Physical documents
☐	Other

How will data be stored and kept safe? Provide details for each type of data (e.g. raw data, contact lists, consent documents, anonymized data, recordings and images, electronic data and paper documents). (Detailed instructions, Example)

Audio-data will be stored on a password-protected USB key in the PI's locked cabinet. It will be deleted from the USB key when data has been verified (i.e., comparing the audio data and transcription) and de-identified. Transcribed and de-identified data will be saved on a password-protected USB key.

9E **Data Disposition (after the project)**

☒	Stored
☐	De-identified data shared publicly
☐	Identifiable data shared publicly
☒	All identifiers/codes will be permanently deleted
☐	Returned to participants
☐	Destroyed

After project completion, describe whether and how the data will be stored for future use. If shared, with whom? If made public, how (e.g. online)? If archived, provide details. Describe any restrictions on access. Will personal identifiers be deleted and when? If data will be destroyed, when? Will participant contact information be kept for future recruitment? (Include data disposition plans in the consent materials) (Detailed instructions, Example)

Anonymized data will be stored for possible future work on the same topic. Data will be stored on password-protected USB key. Identifiable data (audio recordings and participant name/email will be destroyed after approximately one month of the the transcription).

9F **Sharing Study Results**

☐	Results will be shared

Do you intend to share a report (or summary) of the research findings with participants once the study is complete? If yes, include this option in the consent form. (Detailed instructions, Example)

N/A

9G **Data Breach Risks**

☐	No Risks

Describe the likelihood of a data breach and the resulting risks to participants. If risks are significant, how will they be mitigated? (Detailed instructions, Example)

A data breach is unlikely to cause any damage because the data is coded. Besides, we will not ask the participants to share their passwords with us at any stage of our study. However, the study involves mild social/economic risk to participants, and we anticipate mild risks if a breach occurs.

10. Funding and Approvals

10A **Project Funding**

☐	Unfunded

Who is funding this project? If applicable, include the funding source/agency/company, program, award name, and number (from CUResearch). Note if the researcher applied for a release of funds

☒	Tri-Council Funded
☐	Other Award/Grant
☐	Contract Funded
☐	Personal Consulting or Personal Work
☐	Scholarship

for this project funding.

NSERC Discovery Grant #111747: Cognition-Informed Authentication

10B Researcher Funding (for research contracts and personal consulting only)

☒	Not contract funded research
☐	No funds are paid directly to the researcher as personal income
☐	The researcher will receive a portion of the funds as personal income
☐	A copy of the contract/agreement has been submitted to the Research Compliance Office

For research that will pay personal income to any researcher: how will any resulting conflicts of interest be managed? How much funding (dollar amount and the percentage of the total) will the researcher(s) receive as income? Provide the title and date of any contracts. (The REB may review the contract.)

N/A

10C Additional Approvals Required

☒	No other approvals required
☐	Organizational Permission
☐	Visa/Travel Permits
☐	Other REBs or Institutional Approvals
☐	Biohazards
☐	Animal Care Committee
☐	Permission letters attached
☐	Letters to follow
☒	Other (please specify)

Is organizational permission required to conduct research (e.g., schools, employers, other universities, correctional services, indigenous communities, or other data collection locations)? If conducting research in another country, is local permission, including local ethics review, required? Indicate if permission/approval has been secured and provide a copy. Research with biohazards or animals must also secure approval from the appropriate committee at Carleton University.

Recruitment materials will be distributed to the lead researcher's previous university in Bangladesh but no REB clearance is required. They will be only putting up the recruitment posters/letters but we will be conducting the recruitment ourselves.

10D TCPS Tutorial

☒	Completed the online TCPS tutorial
☐	Have not completed the online TCPS tutorial

TCPS CORE Tutorial training is required for all researchers listed on the protocol. Justify any cases where researchers have not completed the TCPS tutorial.

Completed the TCPS tutorial.

11. Declarations

Supervisor Approval

11A

☐	Not applicable
☒	Supervisor Approved

For student projects, please indicate the date that the supervisor approved the application. Such approval indicates that the supervisor has read the entire submission and associated documentation, and is satisfied that the project is appropriately prepared and meets applicable disciplinary and ethical standards. (Detailed instructions, Example)

Supervisor approved the application on November 23, 2020. Prof. Stobert signed the supervisor signature form (See Attachment: Supervisor Signature Form-Appendix#1). She will also be copied on all correspondence with the REB.

Declaration #1

11B

☒	I agree

This ethics application accurately describes the research project or scholarly activity that I plan to conduct. (Detailed instructions, Example)

Declaration #2

11C

☒	I agree

No recruitment or data collection for this protocol will commence before ethics clearance. (Detailed instructions, Example)

Declaration #3

11D

☒	I agree

No changes will be made to the research project as described in this protocol without receiving clearance from the Research Ethics Board. (Detailed instructions, Example)

Declaration #4

11E

☒	I agree

The Research Ethics Board will be notified immediately of any alleged or real ethical breaches or concerns, adverse events, or participant complaints that arise during or after the course of this research project. (Detailed instructions, Example)

12. Comments

Comments (optional)

12A

Do you have any comments or suggestions on the form?

No.

Carleton UNIVERSITY
Canada's Capital University

Recruitment Poster

Participate in a study on
Cultural factors in Password Sharing: A Case Study of Bangladesh

This project is on understanding the cultural sensitivity lying behind password sharing attitudes in Bangladesh.

To participate in this study, you must be:

- ✓ **Bangladeshi**
- ✓ **Comfortable using technology devices, including computer/mobile phones**
- ✓ **At least 18 years old**
- ✓ **Comfortable in either English or Bangla language**

This is a 60-minute study. You will have to complete a pre-screening survey for checking your eligibility. If you are successful, you will be invited to participate in our Zoom interview where you will be asked to share your beliefs and practices related to password sharing.

Participation in this study is voluntary, and you may skip any questions that you wish, and/or withdraw at any time during the interview. All interviews will be audio-recorded.

If you choose to withdraw, all the information you have provided will be destroyed. BDT 1000 compensation will be e-transferred to your bank/bKash account for participating in the interview. You will not be compensated for filling out the pre-screening survey.

This study has been cleared by the Carleton University Research Ethics Board B (Clearance # 114925).

Please contact the researcher, Aniqa Binte Alam, for more details on this study at aniqa.bintealam@carleton.ca.

Carleton UNIVERSITY
Canada's Capital University

Letter of Invitation to University/Company Announcement

Title: Cultural Factors in Password Sharing: A Case Study of Bangladesh

Funding Source: The Natural Sciences and Engineering Research Council of Canada (NSERC) Discovery Grant #111747: Cognition-Informed Authentication

Date: TBD

Hello,

My name is Aniqa Binte Alam and I am a Master's student in the School of Computer Science at Carleton University. I am working on a research project under the supervision of Prof. Elizabeth Stobert.

I am writing to you today to invite you to participate in a study on password sharing practices in Bangladeshi culture. This study aims to increase passwords' usability and minimize security threats caused by password sharing by incorporating relevant culture-specific practices in authentication design. We will not ask you to share your passwords at any stage of our studies.

This study involves a pre-screening survey for checking eligibility and one 60 minutes online interview that will take place in Zoom. To participate in the pre-screening survey, the participants must be at least eighteen years of age and must speak English or Bangla fluently. They must use technology devices, including computer/mobile phones, may use the internet and social media, and may have previous password sharing experiences. We will analyze the pre-screening survey responses and invite suitable candidates for the final interview. The interview can be in Bangla or English. Participation in this study is voluntary, and you may skip any questions that you wish during the interview. All interviews will be audio-recorded. If you do not consent to being audio-recorded you will not be eligible for the study. Once the recording has been transcribed, the audio-recording will be destroyed.

While this project does not involve any professional and emotional risks, care will be taken to protect your identity. This will be done by keeping all responses anonymized.

You may withdraw from this study at any time up to the end of the interview session. If you do choose to withdraw, you will still be compensated, and all data will be deleted from the study. BDT 1000 compensation will be provided for participating in the interview. The compensation will be sent (e-transferred) to your bank account/mobile banking account (bKash). The withdrawal will not have any impact on the compensation.You will not be compensated for filling out the pre-screening survey.

All research data, including audio-recordings and any notes will be kept on a password protected USB key. Any hard copies of data including handwritten notes, USB keys, etc. will be kept in a locked cabinet. Research data will only be accessible by the researcher and the research supervisor.

This research has been cleared by Carleton University Research Ethics Board-B (CUREB-B Clearance # 114925).

Should you have any ethical concerns with the study, please contact the REB Chair, Carleton University Research Ethics Board-B by email: ethics@carleton.ca. For all other questions about the study, please contact the researcher.

If you would like to participate in this research project, or have any questions about the research, please contact me at aniqa.bintealam@carleton.ca.

Sincerely,

Aniqa Binte Alam

Carleton UNIVERSITY
Canada's Capital University

Email Invitation for Interview

Dear XXX,

Thank you for your interest in this study! You are eligible for this study and we are looking forward to your participation. Instructions that require your action in this email are underlined.

Study Introduction:

Passwords are designed to be inherently private and confidential; therefore, password policies strictly forbid to share passwords with anyone. But previous studies have shown that passwords "need" to be shared to accommodate culture-specific practices in some eastern cultures. In this research project, we will try to understand the cultural sensitivity lying behind password sharing attitudes in Bangladesh.

If you agree to take part in the study, we will ask you to attend an one hour long interview on Zoom where you be asked about your password sharing behaviours. It is important that you are alone while giving the interview in order to preserve the privacy of the interview. This is to mention that, we will not ask your passwords at any stages of our study. The interview can be in Bangla or in English according to your preference. Participation in this study is voluntary, and you may skip any questions that you wish during the interview. All interviews will be audio-recorded. If you do not consent to being audio-recorded you will not be eligible for the study.

You may withdraw from this study at any time up to the end of the interview session. If you do choose to withdraw, you will still be compensated, and all data will be deleted from the study. BDT 1000 compensation will be provided for participating in the interview. You will not be compensated for filling out the pre-screening survey.

This research has been cleared by Carleton University Research Ethics Board-B (CUREB-B Clearance # 114925).

Study Timeline:

1. Sign consent form
2. Schedule the interview
3. Inform either bank/bKash account information via email
4. Remote final interview and study debrief *(approx. 60 minutes)*

Upon completion of the interview, you will receive 1000 BDT for your time.

Consent Form:

To access the consent form, please chick here: https://carletonu.az1.qualtrics.com/XXXX. Please read through it carefully, and then sign digitally. This step must be completed before scheduling the interview appointment.

Schedule time for interview session:

We'll need to schedule a time for our final interview session on Zoom. During this time, I'll ask you few questions related to your password sharing behaviour. The session will take approximately 60 minutes. Please choose a time slot that works for you here: https://calendly.com/XXXXXX.

Bank/bKash Account information:

BDT 1000 compensation will be provided for participating in the interview. The compensation will be sent (e-transferred) to your bank account or mobile banking account. If you want the compensation to be

sent to your bank account, please send us in a seperate email (email title: Your name_Password Sharing) your name, bank account number, bank account name, bank name and bank branch name. If you want a bKash transfer, please send us your account name and bKash account phone number via email.

We will maintain a master file with user's name, account number and the confirmation email of the money receipt. The master file will be stored in a password-protected pendrive, which will only be accessible by the researchers.

If you have any questions about any of the above, feel free to email me at any time.

Regards,

Aniqa Binte Alam

MCS in Human Computer Interaction, Carleton University

Carleton UNIVERSITY
Canada's Capital University

Online Invitation

To be posted on Facebook:

Volunteers needed for a study on "Cultural Factors in Password Sharing: A Case Study of Bangladesh"

We are looking for 50 volunteers for an online study. This study aims to increase passwords' usability and minimize security threats caused by password sharing by incorporating relevant culture-specific practices in authentication design. This study involves a pre-screening survey for checking eligibility and one 60 minutes online interview that will take place in Zoom. The interview can be in Bangla or in English.

The study aims to understand password sharing attitudes of Bangladeshi people. You will be asked several questions regarding your understanding, belief and practices related to password sharing. We will not ask you to share your passwords at any stage of our studies.

To be eligible, you must be a Bangladeshi and at least 18 years old, must speak English or Bangla fluently and have sufficient experience with technology devices. You need to fill out the pre-screening survey first. Eligible participants will be invited to participate in an online interview session.

This interview will take place online and should take 60 minutes to complete. The interview can be in Bangla or in English. Participation in this study is voluntary, and you may skip any questions that you wish during the interview. All interviews will be audio-recorded. If you do not consent to being audio-recorded you will not be eligible for the study. Once the recording has been transcribed, the audio-recording will be destroyed.

You may withdraw from this study at any time up to the end of the interview session. If you do choose to withdraw, you will still be compensated, and all interview/survey data will be deleted from the study. BDT 1000 compensation will be provided for participating in the interview. The compensation will be sent (e-transferred) to your bank account/mobile banking account (bKash). The withdrawal will not have any impact on the compensation. You will not be compensated for filling out the pre-screening survey.

If you are interested, please fill out the online pre-screening survey at XXXXXXXXX or email Aniqa Binte Alam at aniqa.bintealam@carleton.ca for more details on participating.

This research has been cleared by Carleton University Research Ethics Board-B (Clearance # 114925).

All research data, including audio-recordings and any notes will be kept on a password protected USB key. Any hard copies of data including handwritten notes, USB keys, etc. will be kept in a locked cabinet. Research data will only be accessible by the researcher and the research supervisor.

Should you have any ethical concerns with the study, please contact the REB Chair, Carleton University Research Ethics Board-B by email: ethics@carleton.ca. For all other questions about the study, please contact the researcher.

Carleton UNIVERSITY
Canada's Capital University

Email Invitation

Subject: Invitation to participate in a research project on Cultural factors in Password Sharing: A Case Study of Bangladesh

Date: TBD

Hello,

My name is Aniqa Binte Alam and I am a Master's student in the School of Computer Science at Carleton University. I am working on a research project under the supervision of Prof. Elizabeth Stobert.

I am writing to you today to invite you to participate in a study on password sharing practices in Bangladeshi culture. This study aims to increase passwords' usability and minimize security threats caused by password sharing by incorporating relevant culture-specific practices in authentication design. We will not ask you to share your passwords at any stage of our studies.

This study involves a pre-screening survey for checking eligibility and one 60 minute online interview that will take place on Zoom. To participate in the pre-screening survey, the participants must be at least eighteen years of age and must speak English or Bangla fluently. They must use technology devices, including computer/mobile phones, may use the internet and social media, and may have previous password sharing experiences. We will analyze the pre-screening survey responses and invite suitable candidates for the final interview. The interview can be in Bangla or English. Participation in this study is voluntary, and you may skip any questions that you wish during the interview. All interviews will be audio-recorded. If you do not consent to being audio-recorded you will not be eligible for the study. Once the recording has been transcribed, the audio-recording will be destroyed.

While this project does not involve any professional or emotional risks, care will be taken to protect your identity. This will be done by keeping all responses anonymized.

BDT 1000 compensation will be e-transferred to your bank/bKash account for participating in the interview. You may withdraw from this study at any time up to the end of the interview session. If you do choose to withdraw, you will still be compensated, and all interview/survey data will be deleted from the study.You will not be compensated for filling out the pre-screening survey.

All research data, including audio-recordings and any notes will be kept on a password protected USB key. Any hard copies of data including handwritten notes, USB keys, etc. will be kept in a locked cabinet. Research data will only be accessible by the researcher and the research supervisor.

This research has been cleared by Carleton University Research Ethics Board-B (Clearance # 114925).

Should you have any ethical concerns with the study, please contact the REB Chair, Carleton University Research Ethics Board-B by email: ethics@carleton.ca. For all other questions about the study, please contact the researcher.

If you would like to participate in this research project, or have any questions about the research, please contact me at aniqa.bintealam@carleton.ca.

Sincerely,

Aniqa Binte Alam

Carleton UNIVERSITY
Canada's Capital University

Email Invitation for Ineligible Participants

Dear XXX,

Thank you for your interest in this study titled "Cultural factors in Password Sharing: A Case Study of Bangladesh"! Unfortunately, we cannot invite you to participate in our interview session.

We highly appreciate your interest and time for the study. If you have any queries, feel free to let me know at aniqa.bintealam@carleton.ca.

Regards,

Aniqa Binte Alam

MCS in Human Computer Interaction

Carleton University

Carleton UNIVERSITY
Canada's Capital University

DEBRIEFING

Name and Contact Information of Researchers:

Aniqa Alam, School of Computer Science, Carleton University

Email: aniqa.bintealam@carleton.ca

Supervisor and Contact Information:

Dr. Elizabeth Stobert, School of Computer Science, Carleton University.

Email: elizabeth.stobert@carleton.ca

Project Title

Cultural Factors in Password Sharing: A Case Study of Bangladesh

Project Sponsor and Funder (if any)

The Natural Sciences and Engineering Research Council of Canada (NSERC) Discovery Grant #111747: Cognition-Informed Authentication

Carleton University Project Clearance

Clearance #: 114925 Date of Clearance: 17 February 2021

What are we trying to learn in this research?

This research examines the culture-specific practices related to password sharing attitudes in Bangladesh. You were invited to complete the pre-screening survey because you were at least eighteen years of age, must speak English or Bangla fluently, and must use technology devices, including computer/mobile phones. The pre-screening questionnaires you completed before this interview assessed your demography and level of experience with password sharing. The interview that you completed tried to find out cultural sensitivity, values and norms that shaped your password sharing behavior. We also asked you to provide information on the coping strategies you typically use to share password in different situations.

We are interested in learning if cultural norms are underrepresented in authentication design and how to address these issues for better usability. We are also interested in determining the problems that the users from different background (e.g., age, education, gender etc.) face related to password sharing.

Why is this important to scientists or the general public?

Passwords are designed to be inherently private and confidential; therefore, password policies strictly forbid to share passwords with anyone. But previous studies have shown that passwords "need" to be shared to accommodate culture-specific practices in some cultures. In this research project, we are trying to understand the cultural sensitivity lying behind password sharing attitudes in Bangladesh.

When password sharing is not permitted by design and policy, but it is a necessity, people usually share their passwords for banking, social media, and entertainment accounts following unsecured procedures:

Carleton UNIVERSITY
Canada's Capital University

writing them down on paper, sending them through SMS, email, and social media. Such unsecured practices can result in credential fraud, account compromise, monetary loss, and cyberbullying. In this project, we want to increase passwords' usability and minimize security threats caused by password sharing by incorporating relevant culture-specific practices in authentication design.

What are our hypotheses and predictions?

We predict that people share passwords for several culture specific reasons despite password policy that strictly forbids doing so. We also predict that age, gender, education and occupation may have an impact on password sharing attitudes and perception.

Where can I learn more?

There have been a few previous works on password sharing. Please find some references below:

[1] Deena Alghamdi, Ivan Flechais, and Marina Jirotka. 2015. Security Practices for Households Bank Customers in the Kingdom of Saudi Arabia. In Eleventh Symposium On Usable Privacy and Security (SOUPS 2015). 297–308.

[2] Joseph Jofish' Kaye. 2011. Self-reported password sharing strategies. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM, 2619–2622.

[3] Supriya Singh, Anuja Cabraal, Catherine Demosthenous, Gunela Astbrink, and Michele Furlong. 2007. Password sharing: implications for security design based on social practice. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM, 895–904.

What if I have questions later?

If you have any remaining concerns, questions, or comments about the experiment, please feel free to contact Aniqa Alam (Principal Investigator), at: aniqa.bintealam@carleton.ca, Dr. Elizabeth Stobert (Faculty Sponsor), at: elizabeth.stobert@carleton.ca.

If you have any ethical concerns with the study, please contact the Carleton University Research Ethics Board-B by email at ethics@carleton.ca.

Thank you for participating in this research!

Carleton UNIVERSITY
Canada's Capital University

Research Consent Text for Survey – Bangla (online)

সমীক্ষার জন্য সম্মতি পাঠ্য - বাংলা (অনলাইন)

গবেষকদের নাম ও যোগাযোগের তথ্য: অনিকা বিনতে আলম, কম্পিউটার সায়েন্স, কার্লটন বিশ্ববিদ্যালয়; ইমেল: aniqabintealam@cmail.carleton.ca

সুপারভাইজার এবং যোগাযোগের তথ্য: ডঃ এলিজাবেথ স্টোবার্ট, কম্পিউটার সায়েন্স, কার্লটন বিশ্ববিদ্যালয়; ইমেল: elizabethstobert@cunet.carleton.ca

প্রকল্পের শিরোনাম: পাসওয়ার্ড শেয়ার এর উপর সাংস্কৃতির প্রভাব : বাংলাদেশের উপর একটি কেস স্টাডি (Cultural Factors in Password Sharing: A Case Study of Bangladesh)

প্রকল্পের পৃষ্ঠপোষক এবং তহবিলকারী: কানাডার ন্যাচারাল সায়েন্সেস এবং ইঞ্জিনিয়ারিং রিসার্চ কাউন্সিল (এনএসইআরসি) আবিষ্কার গ্রান্ট # ১১১৭৪৭

কার্লেটন বিশ্ববিদ্যালয় প্রকল্প ছাড়পত্র:

CUREB-B ছাড়পত্র # ১১৪৯২৫ (115924) ছাড়পত্রের তারিখ: টিবিডি

আমন্ত্রণ

অধ্যয়নের জন্য আপনার যোগ্যতা নির্ধারণ করতে আমরা আপনাকে প্রাক-স্ক্রিনিং সমীক্ষাটি সম্পূর্ণ করতে বলছি। আপনার বয়স কমপক্ষে আঠারো বছর হতে হবে এবং অবশ্যই ইংরেজী বা বাংলা অনর্গল কথা বলতে হবে। আপনাকে অবশ্যই কম্পিউটার / মোবাইল ফোন সহ প্রযুক্তিগত ডিভাইসগুলি ব্যবহার করতে হবে, ইন্টারনেট এবং সোশ্যাল মিডিয়া ব্যবহার করতে পারতে হবে এবং পাসওয়ার্ড শেয়ার করার আগের অভিজ্ঞতা থাকতে পারে। এই সমীক্ষাটি কার্লটন বিশ্ববিদ্যালয়, কম্পিউটার বিজ্ঞান বিভাগের অধ্যাপক এলিজাবেথ স্টোবার্টের তত্ত্বাবধানে কাজ করে (ইমেল: elizabeth stobert@cunet.carleton.ca) কার্লটন বিশ্ববিদ্যালয়, কম্পিউটার বিজ্ঞান বিভাগের আনিকা বিনতে আলম (ইমেল: aniqabintealam@cmail.carleton.ca) দ্বারা পরিচালিত হচ্ছে)।

উদ্দেশ্য এবং সংক্ষিপ্তসার

পাসওয়ার্ড অন্তর্নিহিতভাবে ব্যক্তিগত এবং গোপনীয় হিসাবে ডিজাইন করা হয়েছে; অতএব, পাসওয়ার্ড নীতিগুলি কারও সাথে পাসওয়ার্ড শেয়ার করতে কঠোরভাবে নিষেধ করে। তবে পূর্ববর্তী গবেষণাগুলিতে দেখা গেছে যে কিছু সংস্কৃতিতে সংস্কৃতি-নির্দিষ্ট অনুশীলনের জন্য পাসওয়ার্ডগুলি শেয়ার করা "প্রয়োজনীয়" । এই গবেষণা প্রকল্পে, আমরা বাংলাদেশে পাসওয়ার্ড শেয়ার করার মনোভাবের পিছনে থাকা সাংস্কৃতিক সংবেদনশীলতা বোঝার চেষ্টা করব।

এই জরিপের উদ্দেশ্যটি হল আমাদের মূল গবেষণায় অংশ নেওয়ার জন্য যোগ্যতার মূল্যায়ন করা। সফল প্রার্থীদের ইমেলের মাধ্যমে মূল সাক্ষাৎকারে অংশ নিতে আমন্ত্রিত করা হবে। আমাদের অনুমান যে সমীক্ষাটি শেষ হতে প্রায় ৫ মিনিট সময় লাগবে।

আপনি জরিপ জমা দেওয়ার পরে যদি আপনি প্রত্যাহারের সিদ্ধান্ত নেন, আপনি সমীক্ষার জমা দেওয়ার ২ দিনের মধ্যে

আপনি যদি গবেষককে অবহিত করেন তবে আমরা জরিপ তথ্য থেকে আপনার প্রতিক্রিয়াগুলি সরিয়ে দেব। আমরা অবিলম্বে জরিপ অংশগ্রহণকারীদের ডেটা মুছে ফেলব যাদের সাক্ষাৎকারে আমন্ত্রিত করা হবে না।

আমরা প্রাক-স্ক্রিনিং জরিপ এ পাওয়া তথ্য বিশ্লেষণ করব এবং চূড়ান্ত সাক্ষাৎকারের জন্য উপযুক্ত প্রার্থীদের আমন্ত্রণ করব। সাক্ষাৎকারটি বাংলা বা ইংরেজি হতে পারে। এই গবেষণায় অংশ নেওয়া স্বেচ্ছাসেবী এবং আপনি সাক্ষাৎকারের সময় আপনার যে কোনও প্রশ্ন বাদ দিতে পারেন। সমস্ত সাক্ষাৎকার অডিও রেকর্ড করা হবে। আপনি অডিও-রেকর্ড হতে সম্মতি না দিলে আপনি অধ্যয়নের জন্য যোগ্য নন।

ঝুঁকি এবং উপকারিতা

সমীক্ষা গ্রহণ থেকে আমরা কোনও ঝুঁকি নিয়ে প্রত্যাশা করি না, বা আমরা আশা করি না যে আপনি কোনও উপকার পাবেন।

সম্মানী

এই সমীক্ষায় আপনার অংশগ্রহণ স্বেচ্ছাসেবী এবং আপনি অংশ না নেওয়ার বা কোনও প্রশ্নের উত্তর না দেওয়া বেছে নিতে পারেন। প্রাক-স্ক্রিনিং জরিপ পূরণের জন্য আপনাকে সম্মানী দেওয়া হবে না।

গোপনীয়তা এবং ডেটা স্টোরেজ

আমরা আপনার ব্যক্তিগত তথ্যকে গোপনীয় হিসাবে বিবেচনা করব, যদিও নিখুঁত গোপনীয়তার গ্যারান্টি দেওয়া যায় না। আপনার পরিচয় প্রকাশ করে এমন কোনও তথ্য আপনার নির্দিষ্ট সম্মতি ছাড়া প্রকাশ করা হবে না। চলমান নৈতিকতা সম্মতি নিশ্চিত করার জন্য কার্লেটন বিশ্ববিদ্যালয় গবেষণা নীতিশাস্ত্র কর্তৃক গবেষণা রেকর্ড অ্যাক্সেস করা যেতে পারে। আপনার ডেটা কোয়েলট্রিক্স (সার্ভার টরন্টোতে অবস্থিত) দ্বারা সংরক্ষণ এবং সুরক্ষিত হবে, তবে আদালতের আদেশ বা ডেটা লঙ্ঘনের মাধ্যমে প্রকাশ করা যেতে পারে। এই অধ্যয়নের ফলাফল প্রকাশিত হতে পারে, তবে তথ্য উপস্থাপন করা হবে যাতে এটি আপনাকে সনাক্ত করা সম্ভব না হয়। সমস্ত গবেষণা ডেটা পাসওয়ার্ড-সুরক্ষিত ইউএসবি ড্রাইভে রাখা হবে।

আরইবি পর্যালোচনা এবং যোগাযোগের তথ্য

এই গবেষণাটি কার্লটন বিশ্ববিদ্যালয় গবেষণা নীতিশাসন বোর্ড-বি দ্বারা সরিয়ে দেওয়া হয়েছে (CUREB -B ক্লিয়ারেন্স # ১১৪৯২৫)। অধ্যয়নের সাথে যদি আপনার কোনও নৈতিক উদ্বেগ থাকে তবে দয়া করে Ethics@carleton.ca- এ ইমেল করে কার্লটন বিশ্ববিদ্যালয় গবেষণা নীতিশাস্ত্র বোর্ডের সাথে যোগাযোগ করুন।

নিহিত সম্মতি

অনলাইন সমীক্ষা সমাপ্ত করে, আপনি গবেষণায় অংশ নিতে সম্মত হচ্ছেন।

সরাসরি সম্মতি

আমি স্বেচ্ছায় এই গবেষণায় অংশ নিতে সম্মত।

- ☐ আমি সম্মতি, অধ্যয়ন শুরু করা হোক
- ☐ আমি সম্মতি দিচ্ছি না, আমি অংশ নিতে চাই না

Carleton UNIVERSITY
Canada's Capital University

Informed Consent Form

সম্মতি ফর্ম

গবেষকদের নাম ও যোগাযোগের তথ্য: অনিকা বিনতে আলম, কম্পিউটার সায়েন্স, কার্লটন বিশ্ববিদ্যালয়; ইমেল: aniqabintealam@cmail.carleton.ca

সুপারভাইজার এবং যোগাযোগের তথ্য: ডঃ এলিজাবেথ স্টোবার্ট, কম্পিউটার সায়েন্স, কার্লটন বিশ্ববিদ্যালয়; ইমেল: elizabethstobert@cunet.carleton.ca

প্রকল্পের শিরোনাম: পাসওয়ার্ড শেয়ার এর উপর সাংস্কৃতির প্রভাব : বাংলাদেশের উপর একটি কেস স্টাডি (Cultural Factors in Password Sharing: A Case Study of Bangladesh)

প্রকল্পের পৃষ্ঠপোষক এবং তহবিলকারী: কানাডার ন্যাচারাল সায়েন্সেস এবং ইঞ্জিনিয়ারিং রিসার্চ কাউন্সিল (এনএসইআরসি) আবিষ্কার গ্রান্ট # ১১১৭৪৭

কার্লেটন বিশ্ববিদ্যালয় প্রকল্প ছাড়পত্র:

CUREB-B ছাড়পত্র # ১১৪৯২৫ (115924) ছাড়পত্রের তারিখ: টিবিডি

আমন্ত্রণ

আপনাকে এই গবেষণা প্রকল্পে অংশ নিতে আমন্ত্রণ জানানো হয়েছে কারণ আপনি একজন বাংলাদেশী, অবশ্যই সাবলীলভাবে ইংরেজি বা বাংলা বলতে পারেন, এবং প্রযুক্তি ডিভাইসগুলির সাথে পর্যাপ্ত অভিজ্ঞতার সাথে কমপক্ষে ১৮ বছর বয়সী হতে হবে। এই ফর্মের তথ্যগুলি আপনাকে আমরা আপনাকে যা জিজ্ঞাসা করছি তা বুঝতে সহায়তা করার জন্য যাতে আপনি এই গবেষণায় অংশ নিতে সম্মত হন কিনা তা আপনি সিদ্ধান্ত নিতে পারেন। এই গবেষণায় আপনার অংশগ্রহণ স্বেচ্ছাসেবী এবং অংশ না নেওয়ার সিদ্ধান্তটি আপনার বিরুদ্ধে কোনওভাবেই ব্যবহার করা হবে না। আপনি এই ফর্মটি পড়ার পরে, এবং অংশ নেওয়ার বিষয়ে সিদ্ধান্ত নেওয়ার পরে, দয়া করে আপনার যা যা প্রশ্ন থাকতে পারে তা জিজ্ঞাসা করুন, আপনার প্রয়োজনমতো সময় নিন এবং নিজের ইচ্ছামত অন্যের সাথে পরামর্শ করুন।

গবেষণা উদ্দেশ্য কি?

পাসওয়ার্ডগুলি অন্তর্নিহিতভাবে ব্যক্তিগত এবং গোপনীয় হিসাবে ডিজাইন করা হয়েছে; অতএব, পাসওয়ার্ড নীতিগুলি কারও সাথে পাসওয়ার্ড ভাগ করতে কঠোরভাবে নিষেধ করে। তবে পূর্ববর্তী গবেষণাগুলিতে দেখা গেছে যে কিছু পূর্ব সংস্কৃতিতে সংস্কৃতি-নির্দিষ্ট অনুশীলনের জন্য পাসওয়ার্ডগুলি "প্রয়োজনীয়" ভাগ করে নেওয়া উচিত shared এই গবেষণা প্রকল্পে, আমরা বাংলাদেশে পাসওয়ার্ড ভাগ করে নেওয়ার মনোভাবের পিছনে থাকা সাংস্কৃতিক সংবেদনশীলতা বোঝার চেষ্টা করব।

আমাকে কী করতে বলা হবে?

আপনি যদি স্টাডিতে অংশ নিতে সম্মত হন তবে আমরা আপনাকে জুমের এক ঘন্টার দীর্ঘ সাক্ষাৎকারে অংশ নিতে বলব যেখানে আপনাকে আপনার পাসওয়ার্ড শেয়ার করে নেওয়ার আচরণ সম্পর্কে জিজ্ঞাসা করা হবে। সাক্ষাৎকারের গোপনীয়তা রক্ষার জন্য সাক্ষাৎকার দেওয়ার সময় আপনি একা থাকা গুরুত্বপূর্ণ। এটি উল্লেখ করার জন্য, আমরা

আমাদের গবেষণার কোনও পর্যায়ে আপনার পাসওয়ার্ড জিজ্ঞাসা করব না। সাক্ষাৎকারটি আপনার পছন্দ অনুযায়ী বাংলা বা ইংরেজিতে হতে পারে। এই গবেষণায় অংশ নেওয়া স্বেচ্ছাসেবী এবং আপনি সাক্ষাৎকারের সময় আপনার যে কোনও প্রশ্ন বাদ দিতে পারেন। সমস্ত সাক্ষাৎকার অডিও রেকর্ড করা হবে। আপনি অডিও-রেকর্ড হতে সম্মতি না দিলে আপনি অধ্যয়নের জন্য যোগ্য হবেন না। সম্মানীর পরিমাণ ই-ট্রান্সফার করার জন্য আমাদের আপনার ব্যাংকিং / বিকাশ অ্যাকাউন্টের তথ্য প্রয়োজন।

ঝুঁকি এবং অসুবিধা

আমরা এই গবেষণায় অংশগ্রহণের জন্য কোনও ঝুঁকি নিয়ে প্রত্যাশা করি না। বাংলাদেশের সামাজিক ও লিঙ্গ নিয়মাবলী বিবেচনা করে পাসওয়ার্ড ভাগাভাগি সম্পর্কিত কিছু বিষয় নিয়ে আলোচনা করার সময় আপনি নিজেকে নিরাপত্তাহীন বোধ করতে পারেন। আমাদের অধ্যয়নের যে কোনও পর্যায়ে আপনাকে আপনার আসল পাসওয়ার্ডগুলি ভাগ করতে বলা হবে না। দয়া করে মনে রাখবেন যে গবেষণাটি স্বেচ্ছাসেবী এবং সাক্ষাৎকারটি গোপনীয় এবং আপনার পরিচয়টি অস্পষ্ট রাখতে কোড করা হবে।

সম্ভাব্য উপকারিতা

আপনি এই গবেষণায় আপনার অংশগ্রহণ থেকে সরাসরি কোনও সুবিধা পাবেন না।

সম্মানী

সাক্ষাৎকারে অংশ নেওয়ার জন্য ১০০০ টাকা ক্ষতিপূরণ দেওয়া হবে। ক্ষতিপূরণটি আপনার ব্যাংক অ্যাকাউন্ট / মোবাইল ব্যাংকিং অ্যাকাউন্টে (ই-ট্রান্সফার) প্রেরণ করা হবে। আপনি এই গবেষণা থেকে সাক্ষাৎকার সেশন শেষ পর্যন্ত যে কোনও সময় সরে যেতে পারেন। আপনি যদি প্রত্যাহার করা চয়ন করেন, তবে আপনাকে এখনও ক্ষতিপূরণ দেওয়া হবে এবং সমস্ত তথ্য অধ্যয়ন থেকে মুছে ফেলা হবে।

আপনার অধিকারে কোন ছাড় নয়

এই ফর্মটিতে স্বাক্ষর করে আপনি কোনও অধিকার ছাড়ছেন না বা গবেষকদের কোনও দায়বদ্ধতা থেকে মুক্তি দিচ্ছেন না।

গবেষণা থেকে সরে আসার উপায়

যদি আপনি সাক্ষাৎকার সেশন চলাকালীন আপনার সম্মতি প্রত্যাহার করেন, আপনার প্রত্যাহারের আগে আপনার কাছ থেকে সংগৃহীত সমস্ত তথ্য বাতিল করা হবে।

গোপনীয়তা

আমরা যত তাড়াতাড়ি সম্ভব অধ্যয়নের ডেটা থেকে সনাক্তকারী সমস্ত তথ্য (যেমন, নাম, ইমেল ঠিকানা ইত্যাদি) সরিয়ে ফেলব, যা সাক্ষাৎকারটি গ্রহণের সাত দিন পরে হবে।

আমরা আপনার ব্যক্তিগত তথ্যকে গোপনীয় হিসাবে বিবেচনা করব, যদিও নিখুঁত গোপনীয়তার গ্যারান্টি দেওয়া যায় না। আপনার পরিচয় প্রকাশ করে এমন কোনও তথ্য আপনার নির্দিষ্ট সম্মতি ছাড়াই প্রকাশ বা প্রকাশ করা হবে না। চলমান

নৈতিকতা সম্মতি নিশ্চিত করার জন্য কার্লেটন বিশ্ববিদ্যালয় গবেষণা নীতিশাস্ত্র বোর্ডের (কুরির বি) গবেষণার রেকর্ডগুলি অ্যাক্সেস করতে পারে।

আইন দ্বারা মুক্তির প্রয়োজন না হলে সমস্ত ডেটা গোপনীয় রাখা হবে (উদাঃ শিশু নির্যাতন, নিজের বা অন্যের ক্ষতি)।

এই অধ্যয়নের ফলাফলগুলি প্রকাশিত হতে পারে বা একটি একাডেমিক সম্মেলন বা সভায় উপস্থাপন করা যেতে পারে, তবে তথ্য উপস্থাপন করা হবে যাতে কোনও অংশগ্রহণকারীকে সনাক্ত করা সম্ভব না হয়।

আমরা নিরীক্ষণের উদ্দেশ্যে আপনার নাম, অ্যাকাউন্টের তথ্য এবং ক্ষতিপূরণ নিশ্চিতকরণ রশিদ সহ একটি মাস্টার ফাইল রাখব। মাস্টার ফাইলটি একটি পাসওয়ার্ড সুরক্ষিত ইউএসবি ডিভাইসে রাখা হবে যা কেবল গবেষকদের দ্বারা অ্যাক্সেসযোগ্য হবে।

আপনাকে একটি কোড বরাদ্দ করা হবে যাতে আপনার পরিচয় আপনি সরবরাহ করা সাক্ষাৎকার / সমীক্ষার ডেটার সাথে সরাসরি যুক্ত না হয়। কোডেড তথ্য সহ সমস্ত অধ্যয়নের ডেটা নিরাপদ কম্পিউটারে একটি পাসওয়ার্ড সুরক্ষিত ফাইলে রাখা হবে।

আপনার সাক্ষাৎকারের অডিও রেকর্ডিং স্থানীয়ভাবে গবেষকের কম্পিউটারে সংরক্ষণ করা হবে। অপারেশন ডেটা, যেমন সভা এবং পারফরম্যান্স ডেটা, মার্কিন যুক্তরাষ্ট্রে অবস্থিত সার্ভারগুলিতে জুম দ্বারা সংরক্ষণ এবং সুরক্ষিত করা হবে তবে এটি আদালতের আদেশ বা ডেটা লঙ্ঘনের মাধ্যমে প্রকাশ করা যেতে পারে। আমরা সংরক্ষণ বা স্থানান্তর করি যে কোনও গবেষণা ডেটা আমরা পাসওয়ার্ডটি সুরক্ষিত করব।

তথ্য ধারণ

অধ্যয়ন সমাপ্ত হওয়ার পরে, আপনার ডি-শনাক্ত করা ডেটা ভবিষ্যতের গবেষণা ব্যবহারের জন্য ধরে রাখা হবে। আমরা অনুলিপি করা ফাইলটি রাখব তবে অধ্যয়নের এক মাস পর অডিও রেকর্ডিং নষ্ট করব। সমস্ত ডেটা পাসওয়ার্ড সুরক্ষিত ইউএসবি কীতে সংরক্ষণ করা হবে।

নীতি পর্যালোচনা

এই গবেষণাটি কার্লটন বিশ্ববিদ্যালয় গবেষণা নীতিশাসন বোর্ড-বি দ্বারা সরিয়ে দেওয়া হয়েছে (CUREB ক্লিয়ারেন্স # ১১৪৯২৫)। অধ্যয়নের সাথে যদি আপনার কোনও নৈতিক উদ্বেগ থাকে তবে দয়া করে ethics@carleton.ca- এ ইমেল করে কার্লটন বিশ্ববিদ্যালয় গবেষণা নীতিশাস্ত্র বোর্ডের সাথে যোগাযোগ করুন।

সম্মতি বিবৃতি - প্রিন্ট এবং সাইন নাম

আমি স্বেচ্ছায় এই গবেষণায় অংশ নিতে সম্মত। ___হ্যাঁ ___ না

আমি সাক্ষাৎকারের সময় অডিও রেকর্ড করাতে সম্মত । ___হ্যাঁ ___না

(দ্রষ্টব্য: অডিও রেকর্ডিং বাধ্যতামূলক)

_____ _____

অংশগ্রহণকারী স্বাক্ষর তারিখ

Research team member who interacted with the participant

আমি অংশগ্রহণকারীকে অধ্যয়নটি ব্যাখ্যা করেছি এবং তাদের যে কোনও এবং সমস্ত প্রশ্নের উত্তর দিয়েছি। অংশগ্রহণকারী বুঝতে এবং সম্মতিতে উপস্থিত হয়েছে। আমি অংশগ্রহণকারীকে তাদের রেফারেন্সের জন্য সম্মতি ফর্মের একটি অনুলিপি সরবরাহ করেছি।

_____ _____

গবেষকের স্বাক্ষর তারিখ

Carleton UNIVERSITY
Canada's Capital University

Recruitment Poster - Bangla

নিয়োগের পোস্টার **-** বাংলা

অংশগ্রহণ করুন

পাসওয়ার্ড শেয়ার এর উপর সাংস্কৃতির প্রভাব : বাংলাদেশের উপর একটি কেস স্টাডি

এই প্রকল্পটি বাংলাদেশে পাসওয়ার্ড শেয়ার করার মনোভাবের পিছনে থাকা সাংস্কৃতিক সংবেদনশীলতা বোঝার জন্য।

এই গবেষণায় অংশ নিতে, আপনাকে অবশ্যইঃ

✓ বাংলাদেশী
✓ কম্পিউটার / মোবাইল ফোন সহ প্রযুক্তি ডিভাইসগুলি ব্যবহার করতে পারেন
✓ কমপক্ষে ১৮ বছর বয়সী
✓ ইংরাজী বা বাংলা ভাষাতে কথা বলতে পারেন

এটি একটি ৬০-মিনিট অধ্যয়ন। আপনার যোগ্যতা যাচাই করার জন্য আপনাকে প্রাক-স্ক্রিনিং সমীক্ষা শেষ করতে হবে। আপনি যদি সফল হন তবে আমাদের জুম সাক্ষাৎকারে অংশ নেওয়ার জন্য আপনাকে আমন্ত্রণ জানানো হবে যেখানে আপনাকে পাসওয়ার্ড ভাগ করে নেওয়ার সাথে সম্পর্কিত আপনার বিশ্বাস এবং অনুশীলনগুলি ভাগ করে নেওয়ার জন্য বলা হবে।

এই গবেষণায় অংশ নেওয়া স্বেচ্ছাসেবী এবং আপনি যে কোনও প্রশ্ন বাদ দিতে পারেন এবং / বা সাক্ষাৎকারের সময় যে কোনও সময় প্রত্যাহার করতে পারেন। সমস্ত সাক্ষাৎকার অডিও রেকর্ড করা হবে।

আপনি যদি প্রত্যাহার করতে চান তবে আপনার সরবরাহ করা সমস্ত তথ্য ধ্বংস হয়ে যাবে। সাক্ষাৎকারে অংশ নেওয়ার জন্য ১০০০ টাকা ক্ষতিপূরণ আপনার ব্যাংক / বিকাশ অ্যাকাউন্টে ই-ট্রান্সফার করা হবে। প্রাক-স্ক্রিনিং জরিপ পূরণের জন্য আপনাকে ক্ষতিপূরণ দেওয়া হবে না।

এই অধ্যয়নটি কার্লেটন বিশ্ববিদ্যালয় গবেষণা নীতিশাস্ত্র বি বি দ্বারা ছাড়পত্র পেয়েছে (ছাড়পত্র # ১১৪৯২৫ | 114925)।

Carleton UNIVERSITY
Canada's Capital University

Letter of Invitation to University/Company Announcement - Bangla
বিশ্ববিদ্যালয় / কোম্পানির ঘোষণাপত্রের আমন্ত্রণপত্র - বাংলা

প্রকল্পের শিরোনাম: পাসওয়ার্ড শেয়ার এর উপর সাংস্কৃতির প্রভাব : বাংলাদেশের উপর একটি কেস স্টাডি (Cultural Factors in Password Sharing: A Case Study of Bangladesh)

প্রকল্পের পৃষ্ঠপোষক এবং তহবিলকারী: কানাডার ন্যাচারাল সায়েন্সেস এবং ইঞ্জিনিয়ারিং রিসার্চ কাউন্সিল (এনএসইআরসি) আবিষ্কার গ্রান্ট # ১১১৭৪৭

কার্লেটন বিশ্ববিদ্যালয় প্রকল্প ছাড়পত্র:

CUREB-B ছাড়পত্র # ১১৪৯২৫ (115924) ছাড়পত্রের তারিখ: টিবিডি

হ্যালো,

আমার নাম আনিকা বিনতে আলম এবং আমি কার্লটন বিশ্ববিদ্যালয়ের স্কুল অফ কম্পিউটার সায়েন্সে মাস্টার্সের ছাত্র। আমি অধ্যাপক এলিজাবেথ স্টোবার্টের তত্ত্বাবধানে একটি গবেষণা প্রকল্পে কাজ করছি। আমি এশিয়ান ইউনিভার্সিটি অফ উইমেনের একটি প্রাক্তন ছাত্র (২০১৬ সালের ব্যাচ) এবং কম্পিউটার সায়েন্স এবং আইসিটিতে আমার স্নাতক ডিগ্রি শেষ করেছি / আমি এসএসএল ওয়্যারলেস লিমিটেডে দু'বছর (২০১৭-২০১৯) প্রযুক্তিগত সমন্বয়কারী হিসাবে কাজ করেছি।

বাংলাদেশী সংস্কৃতিতে পাসওয়ার্ড শেয়ার করার অনুশীলনে একটি গবেষণায় অংশ নিতে আপনাকে আমন্ত্রণ জানাতে আমি আজ আপনাকে লিখছি। এই অধ্যয়নের উদ্দেশ্য পাসওয়ার্ডের ব্যবহারযোগ্যতা বাড়াতে এবং প্রমাণীকরণের নকশায় প্রাসঙ্গিক সংস্কৃতি-নির্দিষ্ট অনুশীলনগুলিকে অন্তর্ভুক্ত করে পাসওয়ার্ড শেয়ার করার কারণে সৃষ্ট সুরক্ষা হুমকিকে হ্রাস করা। আমরা আপনাকে অধ্যয়নের কোনও পর্যায়ে আপনার পাসওয়ার্ডগুলি ভাগ করে নেওয়ার অনুরোধ করব না।

এই গবেষণায় যোগ্যতা যাচাই করার জন্য প্রাক-স্ক্রিনিং জরিপ এবং জুমের মধ্যে ৬০ মিনিটের অনলাইন সাক্ষাৎকার জড়িত। প্রাক-স্ক্রিনিং জরিপে অংশ নিতে, অংশগ্রহণকারীদের কমপক্ষে আঠারো বছর বয়স হতে হবে এবং অবশ্যই ইংরেজী বা বাংলা অনর্গল কথা বলতে হবে। তাদের অবশ্যই কম্পিউটার / মোবাইল ফোন সহ প্রযুক্তির ডিভাইসগুলি ব্যবহার করতে হবে, ইন্টারনেট এবং সোশ্যাল মিডিয়া ব্যবহার করতে পারে এবং পাসওয়ার্ড ভাগ করার আগের অভিজ্ঞতা থাকতে পারে। আমরা প্রাক-স্ক্রিনিং জরিপ প্রতিক্রিয়াগুলি বিশ্লেষণ করব এবং চূড়ান্ত সাক্ষাৎকারের জন্য উপযুক্ত প্রার্থীদের আমন্ত্রণ করব। সাক্ষাৎকারটি বাংলা বা ইংরেজি হতে পারে। এই গবেষণায় অংশ নেওয়া স্বেচ্ছামূলক এবং আপনি সাক্ষাৎকারের সময় আপনার যে কোনও প্রশ্ন বাদ দিতে পারেন। সমস্ত সাক্ষাৎকার অডিও রেকর্ড করা হবে। আপনি অডিও-রেকর্ড হতে সম্মতি না দিলে আপনি অধ্যয়নের জন্য যোগ্য হবেন না। রেকর্ডিং প্রতিলিপি হয়ে গেলে অডিও-রেকর্ডিং নষ্ট করা হবে।

যদিও এই প্রকল্পে কোনও পেশাদার এবং মানসিক ঝুঁকি জড়িত না, আপনার পরিচয় রক্ষার জন্য যত্ন নেওয়া হবে। সমস্ত প্রতিক্রিয়া বেনামে রেখে এটি করা হবে।

আপনি এই গবেষণা থেকে সাক্ষাৎকার সেশন শেষ পর্যন্ত যে কোনও সময় সরে যেতে পারেন। আপনি যদি প্রত্যাহার করা চয়ন করেন, তবে আপনাকে এখনও ক্ষতিপূরণ দেওয়া হবে এবং সমস্ত তথ্য অধ্যয়ন থেকে মুছে ফেলা হবে। সাক্ষাৎকারে অংশ নেওয়ার জন্য ১০০০ টাকা সম্মানী দেওয়া হবে। ক্ষতিপূরণটি আপনার ব্যাংক অ্যাকাউন্ট / মোবাইল ব্যাংকিং অ্যাকাউন্টে (ই-ট্রান্সফার) প্রেরণ করা হবে। প্রত্যাহারের সম্মানীর কোনও প্রভাব ফেলবে না। প্রাক-স্ক্রিনিং জরিপ পূরণের জন্য আপনাকে ক্ষতিপূরণ দেওয়া হবে না।

অডিও-রেকর্ডিং এবং কোনও নোট সহ সমস্ত গবেষণা ডেটা একটি পাসওয়ার্ড সুরক্ষিত ইউএসবি কীতে রাখা হবে। হস্তাক্ষর নোট, ইউএসবি কী ইত্যাদিসহ ডেটাগুলির যে কোনও হার্ড কপি লক মন্ত্রিসভায় রাখা হবে। গবেষণা তথ্য কেবল গবেষক এবং গবেষণা তত্ত্বাবধায়ক দ্বারা অ্যাক্সেসযোগ্য হবে।

এই গবেষণাটি কার্লটন বিশ্ববিদ্যালয় গবেষণা নীতিশাসন বোর্ড-বি দ্বারা সরিয়ে দেওয়া হয়েছে (CUREB -B ক্লিয়ারেন্স # ১১৪৯২৫)। অধ্যয়নের সাথে যদি আপনার কোনও নৈতিক উদ্বেগ থাকে তবে দয়া করে Ethics@carleton.ca- এ ইমেল করে কার্লটন বিশ্ববিদ্যালয় গবেষণা নীতিশাস্ত্র বোর্ডের সাথে যোগাযোগ করুন।

আপনি যদি এই গবেষণা প্রকল্পে অংশ নিতে চান, বা গবেষণা সম্পর্কে কোনও প্রশ্ন করতে চান, তবে অনুগ্রহ করে আমার সাথে aniqa.bintealam@carleton.ca এ যোগাযোগ করুন।

বিনীত,
আনিকা বিনতে আলম

Carleton UNIVERSITY
Canada's Capital University

Email Invitation for Interview – Bangla

সাক্ষাৎকারের জন্য ইমেল আমন্ত্রণ - বাংলা

প্রিয় XXX,

এই গবেষণায় আপনার আগ্রহের জন্য আপনাকে ধন্যবাদ! আপনি এই অধ্যয়নের জন্য যোগ্য এবং আমরা আপনার অংশগ্রহণের জন্য অপেক্ষা করছি। এই ইমেলটিতে আপনার ক্রিয়াকলাপের প্রয়োজনীয় নির্দেশাবলীর উপরে আন্ডারলাইন করা হয়েছে।

অধ্যয়নের ভূমিকা:

পাসওয়ার্ডগুলি অন্তর্নিহিতভাবে ব্যক্তিগত এবং গোপনীয় হিসাবে ডিজাইন করা হয়েছে; অতএব, পাসওয়ার্ড নীতিগুলি কারও সাথে পাসওয়ার্ড ভাগ করতে কঠোরভাবে নিষেধ করে। তবে পূর্ববর্তী গবেষণাগুলিতে দেখা গেছে যে কিছু পূর্ব সংস্কৃতিতে সংস্কৃতি-নির্দিষ্ট অনুশীলনের জন্য পাসওয়ার্ডগুলি "প্রয়োজনীয়" ভাগ করে নেওয়া উচিত shared এই গবেষণা প্রকল্পে, আমরা বাংলাদেশে পাসওয়ার্ড ভাগ করে নেওয়ার মনোভাবের পিছনে থাকা সাংস্কৃতিক সংবেদনশীলতা বোঝার চেষ্টা করব।

আপনি যদি স্টাডিতে অংশ নিতে সম্মত হন তবে আমরা আপনাকে জুমের এক ঘন্টার দীর্ঘ সাক্ষাৎকারে অংশ নিতে বলব যেখানে আপনাকে আপনার পাসওয়ার্ড ভাগ করে নেওয়ার আচরণ সম্পর্কে জিজ্ঞাসা করা হবে। সাক্ষাৎকারের গোপনীয়তা রক্ষার জন্য সাক্ষাৎকার দেওয়ার সময় আপনি একা থাকা গুরুত্বপূর্ণ। এটি উল্লেখ করার জন্য, আমরা আমাদের গবেষণার কোনও পর্যায়ে আপনার পাসওয়ার্ড জিজ্ঞাসা করব না। সাক্ষাৎকারটি আপনার পছন্দ অনুসারে বাংলা বা ইংরেজিতে হতে পারে। এই গবেষণায় অংশ নেওয়া স্বেচ্ছাসেবী এবং আপনি সাক্ষাৎকারের সময় আপনার যে কোনও প্রশ্ন বাদ দিতে পারেন। সমস্ত সাক্ষাৎকার অডিও রেকর্ড করা হবে। আপনি অডিও-রেকর্ড হতে সম্মতি না দিলে আপনি অধ্যয়নের জন্য যোগ্য হবেন না।

আপনি এই গবেষণা থেকে সাক্ষাৎকার সেশন শেষ পর্যন্ত যে কোনও সময় সরে যেতে পারেন। আপনি যদি প্রত্যাহার করা চয়ন করেন, তবে আপনাকে এখনও ক্ষতিপূরণ দেওয়া হবে এবং সমস্ত তথ্য অধ্যয়ন থেকে মুছে ফেলা হবে। সাক্ষাৎকারে অংশ নেওয়ার জন্য ১০০০ টাকা সম্মানী দেওয়া হবে। প্রাক-স্ক্রিনিং জরিপ পূরণের জন্য আপনাকে সম্মানী দেওয়া হবে না।

এই গবেষণাটি কার্লটন বিশ্ববিদ্যালয় গবেষণা নীতিশাসন বোর্ড-বি দ্বারা সরিয়ে দেওয়া হয়েছে (CUREB ক্লিয়ারেন্স # ১১৪৯২৫)।

অধ্যয়নের সময়রেখা:

১ . স্বাক্ষর করুন সম্মতি ফর্ম

২. সাক্ষাৎকারের সময়সূচী করুন

৩. ব্যাংক / বিকাশ অ্যাকাউন্টের তথ্য ইমেলের মাধ্যমে জানান

৪. দূরবর্তী চূড়ান্ত সাক্ষাৎকার এবং অধ্যয়নের সংক্ষিপ্ত বিবরণ (প্রায় ৬০ মিনিট)

সাক্ষাৎকারটি শেষ হলে আপনি আপনার সময়ের জন্য ১০০০ বিডিটি পাবেন।

অনুমতি ফরম:

সম্মতি ফর্মটি অ্যাক্সেস করতে দয়া করে এখানে চিক করুন: https://carletonu.az1.qualtrics.com/XXXX। দয়া করে এটি সাবধানে পড়ুন, এবং তারপরে ডিজিটালি স্বাক্ষর করুন। সাক্ষাৎকার অ্যাপয়েন্টমেন্টের সময় নির্ধারণের আগে এই পদক্ষেপটি সম্পন্ন করতে হবে।

সাক্ষাৎকার সেশনের সময়সূচী:

জুম সম্পর্কে আমাদের চূড়ান্ত সাক্ষাৎকার সেশনের জন্য আমাদের একটি সময় নির্ধারণ করতে হবে। এই সময়ে, আমি আপনাকে আপনার পাসওয়ার্ড ভাগ করে নেওয়ার আচরণ সম্পর্কিত কয়েকটি প্রশ্ন জিজ্ঞাসা করব। সেশনটি প্রায় ৬০ মিনিট সময় নেবে। দয়া করে এমন সময় স্লট চয়ন করুন যা এখানে আপনার জন্য কাজ করে: https://cenderly.com/XXXXXX।

ব্যাংক / বিকাশ অ্যাকাউন্টের তথ্য:

সাক্ষাৎকারে অংশ নেওয়ার জন্য ১০০০ টাকা ক্ষতিপূরণ দেওয়া হবে। ক্ষতিপূরণটি আপনার ব্যাংক অ্যাকাউন্ট বা মোবাইল ব্যাংকিং অ্যাকাউন্টে (ই-ট্রান্সফার) প্রেরণ করা হবে। যদি আপনি ক্ষতিপূরণটি আপনার ব্যাঙ্ক অ্যাকাউন্টে প্রেরণ করতে চান তবে দয়া করে আমাদেরকে আলাদা ইমেইলে (ইমেল শিরোনাম: আপনার নাম_পাসওয়ার্ড শেয়ারিং) আপনার নাম, ব্যাঙ্ক অ্যাকাউন্ট নম্বর, ব্যাঙ্ক অ্যাকাউন্টের নাম, ব্যাঙ্কের নাম এবং ব্যাংকের শাখার নাম প্রেরণ করুন। আপনি যদি বিকাশ স্থানান্তর চান তবে দয়া করে ইমেলের মাধ্যমে আমাদের আপনার অ্যাকাউন্টের নাম এবং বিকাশ অ্যাকাউন্ট ফোন নম্বর প্রেরণ করুন।

আমরা ব্যবহারকারীর নাম, অ্যাকাউন্ট নম্বর এবং অর্থ প্রাপ্তির নিশ্চিতকরণ ইমেল সহ একটি মাস্টার ফাইল বজায় রাখব। মাস্টার ফাইলটি পাসওয়ার্ড-সুরক্ষিত পেনড্রাইভে সংরক্ষণ করা হবে, যা কেবল গবেষকদের দ্বারা অ্যাক্সেসযোগ্য হবে।

উপরের যে কোনও সম্পর্কে আপনার যদি কোনও প্রশ্ন থাকে তবে যেকোন সময় আমাকে ইমেল করতে দ্বিধা বোধ করবেননা।

শুভেচ্ছা,

আনিকা বিনতে আলম

এমসিএস, হিউম্যান কম্পিউটার ইন্টারেক্টেশন, কার্লেটন বিশ্ববিদ্যালয়

Carleton UNIVERSITY
Canada's Capital University

Online Invitation - Bangla

অনলাইন আমন্ত্রণ - বাংলা

ফেসবুকে পোস্ট করার জন্য:

"পাসওয়ার্ড শেয়ার করার ক্ষেত্রে সাংস্কৃতির অবদান: বাংলাদেশের একটি কেস স্টাডি" শীর্ষক একটি গবেষণার জন্য স্বেচ্ছাসেবীদের প্রয়োজন"

আমরা একটি অনলাইন অধ্যয়নের জন্য ৫০ জন স্বেচ্ছাসেবীর সন্ধান করছি। এই অধ্যয়নের উদ্দেশ্য পাসওয়ার্ডের ব্যবহারযোগ্যতা বাড়াতে এবং প্রমাণীকরণের নকশায় প্রাসঙ্গিক সংস্কৃতি-নির্দিষ্ট অনুশীলনগুলিকে অন্তর্ভুক্ত করে পাসওয়ার্ড ভাগ করে নেওয়ার কারণে সৃষ্ট সুরক্ষা হুমকিকে হ্রাস করা। এই গবেষণায় যোগ্যতা যাচাই করার জন্য প্রাক-স্ক্রিনিং জরিপ এবং জুমের মধ্যে এক ৬০ মিনিটের অনলাইন সাক্ষাৎকার জড়িত। সাক্ষাৎকারটি বাংলা বা ইংরেজিতে হতে পারে।

সমীক্ষাটির লক্ষ্য বাংলাদেশিদের পাসওয়ার্ড শেয়ার করার মনোভাব বোঝা। আপনাকে আপনার বোঝাপড়া, বিশ্বাস এবং পাসওয়ার্ড ভাগ করে নেওয়ার সম্পর্কিত অনুশীলন সম্পর্কিত কয়েকটি প্রশ্ন জিজ্ঞাসা করা হবে। আমরা আপনাকে অধ্যয়নের কোনও পর্যায়ে আপনার পাসওয়ার্ড শেয়ার করার অনুরোধ করব না।

যোগ্য হওয়ার জন্য আপনাকে অবশ্যই বাংলাদেশী হতে হবে এবং কমপক্ষে ১৮ বছর বয়সী হতে হবে, অবশ্যই সাবলীলভাবে ইংরেজি বা বাংলা বলতে হবে এবং প্রযুক্তি ডিভাইসগুলির সাথে পর্যাপ্ত অভিজ্ঞতা থাকতে হবে। আপনাকে প্রথমে প্রাক-স্ক্রিনিং জরিপটি পূরণ করতে হবে। যোগ্য অংশগ্রহণকারীদের একটি অনলাইন সাক্ষাৎকার সেশনে অংশ নিতে আমন্ত্রণ জানানো হবে।

এই সাক্ষাৎকারটি অনলাইনে অনুষ্ঠিত হবে এবং এটি শেষ হতে ৬০ মিনিটের সময় নেওয়া উচিত। সাক্ষাৎকারটি বাংলা বা ইংরেজিতে হতে পারে। এই গবেষণায় অংশ নেওয়া স্বেচ্ছাসেবী এবং আপনি সাক্ষাৎকারের সময় আপনার যে কোনও প্রশ্ন বাদ দিতে পারেন। সমস্ত সাক্ষাৎকার অডিও রেকর্ড করা হবে। আপনি অডিও-রেকর্ড হতে সম্মতি না দিলে আপনি অধ্যয়নের জন্য যোগ্য হবেন না। রেকর্ডিং প্রতিলিপি হয়ে গেলে, অডিও-রেকর্ডিং নষ্ট হয়ে যায়।

আপনি এই গবেষণা থেকে সাক্ষাৎকার সেশন শেষ পর্যন্ত যে কোনও সময় সরে যেতে পারেন। আপনি যদি প্রত্যাহার করা চয়ন করেন, তবে আপনাকে এখনও ক্ষতিপূরণ দেওয়া হবে এবং সমস্ত সাক্ষাৎকার / সমীক্ষার ডেটা অধ্যয়ন থেকে মুছে ফেলা হবে। সাক্ষাৎকারে অংশ নেওয়ার জন্য ১০০০ টাকা সম্মানী দেওয়া হবে। সম্মানীটি আপনার ব্যাংক অ্যাকাউন্ট / মোবাইল ব্যাংকিং অ্যাকাউন্টে (ই-ট্রান্সফার) প্রেরণ করা হবে। প্রত্যাহারের সম্মানীর কোনও প্রভাব পড়বে না। প্রাক-স্ক্রিনিং জরিপ পূরণের জন্য আপনাকে ক্ষতিপূরণ দেওয়া হবে না।

আপনি যদি আগ্রহী হন, তবে অংশগ্রহণের বিষয়ে আরও তথ্যের জন্য অনুগ্রহ করে XXXXXXXXXX- এ অনলাইন প্রাক-স্ক্রিনিং জরিপটি পূরণ করুন বা আনিকা বিনতে আলমকে aniqa.bintealam@carleton.ca এ ইমেল করুন। এই গবেষণাটি কার্লটন বিশ্ববিদ্যালয় গবেষণা নীতিশাসন বোর্ড-বি দ্বারা ছাড়পত্র পেয়েছে (ছাড়পত্র # ১১৪৯২৫)।

অডিও-রেকর্ডিং এবং কোনও নোট সহ সমস্ত গবেষণা ডেটা একটি পাসওয়ার্ড সুরক্ষিত ইউএসবি কীতে রাখা হবে। হস্তাক্ষর নোট, ইউএসবি কী ইত্যাদিসহ ডেটাগুলির যে কোনও হার্ড কপি লক মন্ত্রিসভায় রাখা হবে। গবেষণা তথ্য কেবল গবেষক এবং গবেষণা তত্ত্বাবধায়ক দ্বারা অ্যাক্সেসযোগ্য হবে।

অধ্যয়নের সাথে আপনার যদি কোনও নৈতিক উদ্বেগ থাকে তবে দয়া করে আরইবি চেয়ার, কার্লটন বিশ্ববিদ্যালয় গবেষণা নীতিশাস্ত্র বোর্ড-বি সাথে ইমেলের মাধ্যমে যোগাযোগ করুন: ethics@carleton.ca। গবেষণা সম্পর্কে অন্যান্য সমস্ত প্রশ্নের জন্য, দয়া করে গবেষকের সাথে যোগাযোগ করুন।

Carleton UNIVERSITY
Canada's Capital University

Email Invitation – Bangla

ইমেল আমন্ত্রণ - বাংলা

প্রকল্পের শিরোনাম: পাসওয়ার্ড শেয়ার এর উপর সাংস্কৃতির প্রভাব : বাংলাদেশের উপর একটি কেস স্টাডি (Cultural Factors in Password Sharing: A Case Study of Bangladesh)

প্রকল্পের পৃষ্ঠপোষক এবং তহবিলকারী: কানাডার ন্যাচারাল সায়েন্সেস এবং ইঞ্জিনিয়ারিং রিসার্চ কাউন্সিল (এনএসইআরসি) আবিষ্কার গ্রান্ট # ১১১৭৪৭

কার্লেটন বিশ্ববিদ্যালয় প্রকল্প ছাড়পত্র:

CUREB-B ছাড়পত্র # ১১৪৯২৫ (115924) ছাড়পত্রের তারিখ: টিবিডি

হ্যালো,

আমার নাম আনিকা বিনতে আলম এবং আমি কার্লটন বিশ্ববিদ্যালয়ের স্কুল অফ কম্পিউটার সায়েন্সে মাস্টার্সের ছাত্র। আমি অধ্যাপক এলিজাবেথ স্টোবার্টের তত্ত্বাবধানে একটি গবেষণা প্রকল্পে কাজ করছি।

বাংলাদেশী সংস্কৃতিতে পাসওয়ার্ড শেয়ার করার অনুশীলনে একটি গবেষণায় অংশ নিতে আপনাকে আমন্ত্রণ জানাতে আমি আজ আপনাকে লিখছি। এই অধ্যয়নের উদ্দেশ্য পাসওয়ার্ডের ব্যবহারযোগ্যতা বাড়াতে এবং প্রমাণীকরণের নকশায় প্রাসঙ্গিক সংস্কৃতি-নির্দিষ্ট অনুশীলনগুলিকে অন্তর্ভুক্ত করে পাসওয়ার্ড শেয়ার করার কারণে সৃষ্ট সুরক্ষা হুমকিকে হ্রাস করা। আমরা আপনাকে অধ্যয়নের কোনও পর্যায়ে আপনার পাসওয়ার্ডগুলি ভাগ করে নেওয়ার অনুরোধ করব না।

এই গবেষণায় যোগ্যতা যাচাই করার জন্য প্রাক-স্ক্রিনিং জরিপ এবং জুমের মধ্যে ৬০ মিনিটের অনলাইন সাক্ষাৎকার জড়িত। প্রাক-স্ক্রিনিং জরিপে অংশ নিতে, অংশগ্রহণকারীদের কমপক্ষে আঠারো বছর বয়স হতে হবে এবং অবশ্যই ইংরেজী বা বাংলা অনর্গল কথা বলতে হবে। তাদের অবশ্যই কম্পিউটার / মোবাইল ফোন সহ প্রযুক্তির ডিভাইসগুলি ব্যবহার করতে হবে, ইন্টারনেট এবং সোশ্যাল মিডিয়া ব্যবহার করতে পারে এবং পাসওয়ার্ড ভাগ করার আগের অভিজ্ঞতা থাকতে পারে। আমরা প্রাক-স্ক্রিনিং জরিপ প্রতিক্রিয়াগুলি বিশ্লেষণ করব এবং চূড়ান্ত সাক্ষাৎকারের জন্য উপযুক্ত প্রার্থীদের আমন্ত্রণ করব। সাক্ষাৎকারটি বাংলা বা ইংরেজি হতে পারে। এই গবেষণায় অংশ নেওয়া স্বেচ্ছামূলক এবং আপনি সাক্ষাৎকারের সময় আপনার যে কোনও প্রশ্ন বাদ দিতে পারেন। সমস্ত সাক্ষাৎকার অডিও রেকর্ড করা হবে। আপনি অডিও-রেকর্ড হতে সম্মতি না দিলে আপনি অধ্যয়নের জন্য যোগ্য হবেন না। রেকর্ডিং প্রতিলিপি হয়ে গেলে অডিও-রেকর্ডিং নষ্ট করা হবে।

যদিও এই প্রকল্পে কোনও পেশাদার এবং মানসিক ঝুঁকি জড়িত না, আপনার পরিচয় রক্ষার জন্য যত্ন নেওয়া হবে। সমস্ত প্রতিক্রিয়া বেনামে রেখে এটি করা হবে।

আপনি এই গবেষণা থেকে সাক্ষাৎকার সেশন শেষ পর্যন্ত যে কোনও সময় সরে যেতে পারেন। আপনি যদি প্রত্যাহার করা চয়ন করেন, তবে আপনাকে এখনও ক্ষতিপূরণ দেওয়া হবে এবং সমস্ত তথ্য অধ্যয়ন থেকে মুছে ফেলা হবে। সাক্ষাৎকারে অংশ নেওয়ার জন্য ১০০০ টাকা সম্মানী দেওয়া হবে। ক্ষতিপূরণটি আপনার ব্যাংক অ্যাকাউন্ট / মোবাইল ব্যাংকিং অ্যাকাউন্টে (ই-ট্রান্সফার) প্রেরণ করা হবে। প্রত্যাহারের সম্মানীর কোনও প্রভাব ফেলবে না। প্রাক-স্ক্রিনিং জরিপ পূরণের জন্য আপনাকে ক্ষতিপূরণ দেওয়া হবে না।

অডিও-রেকর্ডিং এবং কোনও নোট সহ সমস্ত গবেষণা ডেটা একটি পাসওয়ার্ড সুরক্ষিত ইউএসবি কীতে রাখা হবে। হস্তাক্ষর নোট, ইউএসবি কী ইত্যাদিসহ ডেটাগুলির যে কোনও হার্ড কপি লক মন্ত্রিসভায় রাখা হবে। গবেষণা তথ্য কেবল গবেষক এবং গবেষণা

তত্ত্বাবধায়ক দ্বারা অ্যাক্সেসযোগ্য হবে।

এই গবেষণাটি কার্লটন বিশ্ববিদ্যালয় গবেষণা নীতিশাসন বোর্ড-বি দ্বারা সরিয়ে দেওয়া হয়েছে (CUREB -B ক্লিয়ারেন্স # ১১৪৯২৫)। অধ্যয়নের সাথে যদি আপনার কোনও নৈতিক উদ্বেগ থাকে তবে দয়া করে Ethics@carleton.ca- এ ইমেল করে কার্লটন বিশ্ববিদ্যালয় গবেষণা নীতিশাস্ত্র বোর্ডের সাথে যোগাযোগ করুন।

আপনি যদি এই গবেষণা প্রকল্পে অংশ নিতে চান, বা গবেষণা সম্পর্কে কোনও প্রশ্ন করতে চান, তবে অনুগ্রহ করে আমার সাথে aniqa.bintealam@carleton.ca এ যোগাযোগ করুন।

বিনীত,
আনিকা বিনতে আলম

Carleton UNIVERSITY
Canada's Capital University

Email Invitation for Ineligible Participants – Bangla

অযোগ্য অংশগ্রহণকারীদের জন্য ইমেল - বাংলা

প্রিয় XXX,

পাসওয়ার্ড শেয়ার এর উপর সাংস্কৃতির প্রভাব : বাংলাদেশের উপর একটি কেস স্টাডি (Cultural Factors in Password Sharing: A Case Study of Bangladesh) শীর্ষক এই গবেষণায় আপনার আগ্রহের জন্য আপনাকে ধন্যবাদ! দুর্ভাগ্যক্রমে, আমরা আপনাকে আমাদের সাক্ষাৎকার সেশনে অংশ নিতে আমন্ত্রণ জানাতে পারি না।

আমরা আপনার আগ্রহ এবং অধ্যয়নের জন্য সময়কে অত্যন্ত প্রশংসা করি। আপনার যদি কোনও প্রশ্ন থাকে তবে নির্দ্বিধায় আমাকে aniqa.bintealam@carleton.ca এ জানান।

শুভেচ্ছা,

আনিকা বিনতে আলম

এমসিএস, হিউম্যান কম্পিউটার ইন্টারঅ্যাকশন

কার্লটন বিশ্ববিদ্যালয়