Social Support for Mobile Security: Comparing Close Connections and Community Volunteers in a Field Experiment

Tamir Mendel
New York University, New York, USA
tm4109@nyu.edu

Eran Toch
Tel Aviv University, Israel
erant@tauex.tau.ac.il

ABSTRACT

People regularly rely on social support from family, friends, and the public when mitigating security and privacy risks, even if mainstream technologies hardly support these interactions. In this paper, we evaluated Meerkat, a mobile application that allows users to receive support through screenshot capturing, marking, and messaging. In a field experiment (n = 65), we tested how Meerkat helps users face phishing attempts and examined it by receiving help from close social connections and community volunteers. Our findings show that while users could learn from both types of helpers, they were significantly more willing to rely on advice from close connections. We evaluate several criteria for successful support interactions, showing that learning is significantly correlated with specific properties of the support interaction, such as the length of the messages. We conclude the paper by discussing how our findings can be used to design community-based applications.

CCS CONCEPTS

• **Security and privacy** → Human and societal aspects of security and privacy; Social aspects of security and privacy; • **Human-centered computing** → Ubiquitous and mobile computing; Empirical studies in ubiquitous and mobile computing.

KEYWORDS

Social support, collective efficacy, security, phishing, mobile

ACM Reference Format:
Tamir Mendel and Eran Toch. 2023. Social Support for Mobile Security: Comparing Close Connections and Community Volunteers in a Field Experiment. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems (CHI '23), April 23–28, 2023, Hamburg, Germany.* ACM, New York, NY, USA, 18 pages. https://doi.org/10.1145/3544548.3581183

1 INTRODUCTION

Mobile technologies have become highly imperative in people's lives for almost any aspect of daily life, including social interactions, work, health, and education. As a result, mobile devices regularly hold sensitive personal information such as the user's location, social contacts, private photos, and payment methods. The COVID-19 pandemic has further steered people's work and social life to mobile technologies [7, 32, 39, 45]. At the same time, the pandemic is also correlated with a dramatic increase in social engineering attacks that include phishing and malware distribution [13, 51]. These attacks are hazardous because they are simple and affordable to run, evade many automated security systems, and rely on simple manipulations that are successful in large-scale campaigns [13].

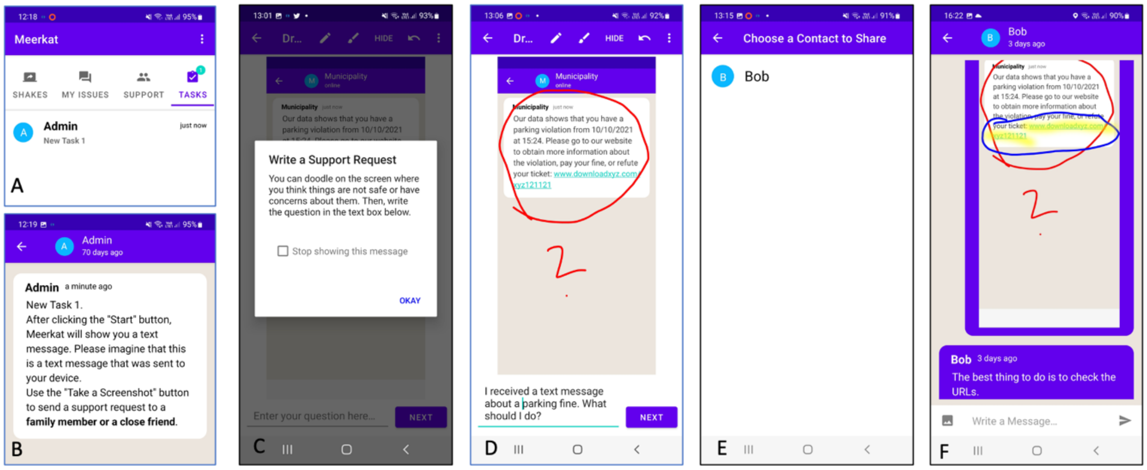
Receiving support is one of the most important ways people cope with social engineering attacks [18, 23]. People regularly rely on family, friends, and community support when learning to use mobile technology [21, 37]. However, HCI researchers only recently started looking at social and collaborative security and privacy aspects [50]. Recent studies have shown that support from close connections can increase users' ability to handle digital technology and enhance their self-efficacy [11, 26, 37]. Recent studies have pointed out that social support has more potential than how it materializes today. People are willing to provide more help than they are being asked: they are eager to assist once a week when the current frequency of helping is once a month [29].

We can divide social support applications into two main categories. The first category is systems that rely on a community of volunteers to provide aid and support. These include communities such as stack overflow and apps that offer safety help. The second category relies on existing social connections and networks. In these systems, users can help people they already know. Previous studies presented applications that support people with close connections. AppMoD is an example of an application that allows older adults to delegate security and privacy decisions to a trusted social contact, such as children or grandchildren [46]. Aljallad et al. presented an application that helps users collaborate with close people to make decisions about application permissions [1]. However, a community of volunteers, people who do not know each other, was not investigated in the context of mobile security and privacy support. Our research questions evaluate the influence of close social connection compared to the community of volunteers through the seeker and helper perceptions of reliance and learning from the social support process.

This paper presents a user study based on **Meerkat**, a mobile application for peer support in Android smartphones (see Figure 1). The app allows users to ask for and receive help when encountering challenging interactions with their mobile phones. Users can have multiple roles: seekers, users who receive technical support, and helpers who provide technical assistance. Meerkat allows seekers to receive support from contacts (e.g., family and friends) or from other users that form a community of volunteers. When users want help, they can capture a screenshot and ask another user for explanations and advice by doodling and writing over the screenshot.

CHI '23, April 23–28, 2023, Hamburg, Germany

ACM ISBN 978-1-4503-9421-5/23/04…$15.00
https://doi.org/10.1145/3544548.3581183



Admin just now
New Task 1

Admin 70 days ago

Admin a minute ago
New Task 1.
After clicking the "Start" button, Meerkat will show you a text message. Please imagine that this is a text message that was sent to your device.
Use the "Take a Screenshot" button to send a support request to a **family member or a close friend.**

Write a Support Request
You can doodle on the screen where you think things are not safe or have concerns about them. Then, write the question in the text box below.
□ Stop showing this message

Enter your question here...

Municipality just now
Our data shows that you have a parking violation from 10/10/2021 at 15:24. Please go to our website to obtain more information about the violation, pay your fine, or refute your ticket: www.downloadxyz.com/xyz121121

I received a text message about a parking fine. What should I do?

Bob

Bob 3 days ago
The best thing to do is to check the URLs.

Figure 1: Screenshots of the Meerkat app. The experiment contains several steps from the viewpoint of a seeker who requests support. (A) The seeker receives a new task in the tasks tab. (B) The seeker sends questions to the helper. (C) The seeker receives guidance to ask the helper where the message is unsafe. (D) The seeker gets a screenshot of the text message. The seeker can draw on the screenshot and write a message to describe and highlight the problem. (E) The seeker can select support and receive support from a user she knows or does not know (in this example, the app randomly assigns the community member). (F) The seeker can see the helper's message with a blue pen on the screenshot and text below the attached screenshot.

In this paper, we describe and present the results of a within-subject design experiment comparing support from close connections and community volunteers providing support against phishing attempts. We analyze participants' interaction support behavior when receiving support from their close connections or community volunteers. This paper contributes to the field of online social safety in the following ways:

- We analyze the seekers' perceptions of reliance on support and learning from it and show that while their perceptions are positive for the two types of helpers, they are significantly higher for close social connection.
- We characterize successful support interactions and show that they are associated with specific aspects of the interaction, such as the number of words the helper uses.
- We analyze the helpers' attitudes and their beliefs in the quality of the support they provide and document that they felt more satisfied when helping close connections.
- We document the association between personal attitudes and abilities of seekers and helpers and show that help is more educational to seekers with lower security awareness.

2 BACKGROUND

2.1 Phishing Attacks

Phishing attacks are quickly becoming one of the more dangerous types of online attacks. In such types of attacks, the attacker usually sends a message with a spoofed URL to a fake website that copies the behavior of a legitimate website. Attackers can collect the client's sensitive data, such as user account login details or other credentials [6]. General, non-specific phishing attacks have a click-through rate of 36% for text messages and 7% for emails [35]. Spear phishing, which uses specific target information, is even more dangerous. Internet users are highly susceptible to spear phishing email attacks, with more than 40% of participants clicking on an email link at least once during the study period [34]. The average open rate of email messages is up to 33%, while the rate for text messages is even higher.

Several solutions for phishing were proposed, with most based on machine learning classification of suspicious messages. Models trained with phishing and non-phishing labels with features such as URLs, HTML content, and SSL certificates [19] or with information about the design of the website [9] reduce the number of phishing messages but do not eliminate them. Machine learning approaches suffer scalability issues and produce high false-positive rates [6]. Moreover, the machine learning approaches cannot identify zero-hour phishing attacks because these techniques depend on the dataset [19].

Given the inherent limitations of automated phishing filtering, educational methods were heavily researched and are commonly used. Increasing users' security awareness, cautiousness, and self-efficacy is crucial to teach users how to identify phishing messages [12]. For example, McElwee et al. revealed that providing repeated and targeted exercises is an excellent way to limit employees' susceptibility to phishing attacks [24]. Games were reported as methods for training users about phishing attacks, such as AntiPhishing [40] and What.Hack [49]. However, social resources are not evenly distributed and are seldom available beyond the organizations' scope. Many vulnerable populations, such as older adults, children, and part-time workers, are left without access to online safety resources. To this end, we look at collective resources available in users' communities and think of ways to enhance the ability of these communities to support individuals.

2.2 Collective Approaches to Online Safety

Most human-centered solutions to combat phishing attacks were focused on increasing users' self-efficacy, defined as a person's belief in their innate ability to perform a particular behavior in various circumstances [2, 3]. However, considering the challenges of cyber-security training, the attention of HCI researchers turns recently been on social aspects of security and privacy [50]. A core idea in thinking about how social relations correspond with safety is Collective Efficacy, the group's shared perception of its capability to perform some behavior successfully [4]. It represents people's shared beliefs that their collective power can produce desired results are critical in collective agency [5]. Collective efficacy was initially developed in urban crime and education, but it can also explain and enhance digital security and privacy [21]. For example, communities of older adults that were more supportive were less vulnerable to mental and health challenges during the Covid-19 pandemic [33]. Kropczynski et al. have shown that enabling connections between low technical ability and people with above-average technical expertise may allow people to increase their security awareness and better manage privacy settings [20]. Murthy et al. document collaborative behaviors enacted by household members and demonstrate how these behaviors can cross the line between digital stewardship and paternalism [31].

Several technologies aim to create collaborative processes, such as providing community oversight over individual privacy choices. Aljallad et al. examined a prototype that helps users collaborate with close connections to decide on accepting application permissions [1]. Chouhan et al. explored a community oversight system that allows users to interact with other users they trust in the context of digital privacy and security. They discovered that participants were willing to provide lightweight passive help to their close connections about online privacy and security decisions, and they did not see themselves doing this daily [8]. Watson et al. examined how social groups (e.g., friends, family, or roommates) share digital resources, showing that social oversight practices protect their resources in making safer decisions [48].

2.3 Peer Support in Security and Privacy

Peer support is one of the main tools to enhance collective efficacy. People regularly rely on mobile security and privacy support from family, friends, and the community [21, 37]. The users' susceptibility to adopt security and privacy behaviors is influenced by their relationship with their peers [28]. Another influential aspect of peer support is social cues, which can make users more likely to adopt the same security behaviors [11]. Social support may encourage conversations with family members about security features, which are critical enablers of a socially driven behavioral change and essential for online safety learning [11, 28]. Peer support can encourage social *learning* when the seeker acquires new knowledge and skills. In the context of security and privacy, social learning allows users to understand the context in which security decisions are made and lead them to higher levels of independence [11]. Family members often provide specialized care to others, advising, guiding, demonstrating, and fixing problems with their mobile phones [29]. Helpers are motivated to help more than they currently do with smartphone security and privacy problems. They are willing to assist with smartphone security and privacy problems once a week when the current frequency of helping is once a month [25].

Several studies have explored peer-support technologies for security and privacy [27, 50]. Wan et al. presented a mobile application that allowed older adults to delegate security decisions to younger family members, measuring their reliance on advice and showing that they made safer decisions in this way [46]. In peer support scenarios, *reliance* reflects the seekers' willingness to follow the helper's decision or recommendation. Higher levels of reliance can help users make more confident choices, but it can also limit their ability to learn new skills and become more independent. For example, in the Wan et al. study, participants neither acquired security-related knowledge nor learned from delegated decisions. Peer support mechanisms need to boost learning and reliance to maximize self-efficacy and collective efficacy. In [26, 30], a peer support prototype was evaluated, providing a conversation-based interface for receiving support and allowing deeper discussions that may foster better learning. In [27], a design for proactive support was suggested to identify the right moment to provide support on mobile smartphones, showing that human behavioral features are essential for the prediction, such as user anxiety, openness to social support, self-efficacy, and security awareness.

Supporting and influencing others' safety can be carried out in interactions with various social scales, ranging from intimate relationships, families and households, social acquaintances, and the public [50]. Several support technologies rely on a community of helpers who register and are willing to support strangers. Community-based technologies were also developed to support urban security and mental health. The SafeUP application contains community members who will support the needed community member and ensure that feels safe, protected, and empowered [42]. Online mental health communities help to manage mental well-being by allowing community members to respond to other users' posts [41]. In the workplace, weak-tie connections may offer helpful advice and solve technical problems thanks to a diversity of skills [10], but in non-workplace environments, helpers tend to provide a lower quality of help to people they do not know well [36]. Helper communities solve some of the inherent challenges of support systems, namely, how to support people that do not have an existing social network that can help them access support resources. At the same time, designing support communities for online safety poses a tricky question: security and privacy are inherently complex concepts that require some understanding and familiarity with people's abilities and preferences.

2.4 Research Questions and Hypotheses

Our primary research objective is to understand how peer support system function with different types of social connections. We divide the peer support system into two main variations: based on the seekers' social network (e.g., [46, 50]) and based on a community of volunteers (e.g., [42]). We evaluate reliance and learning as the central facilitators of support performance for human-human. Based on the concerns users might have with seeking advice [26], we also evaluated how users' concerns with the disclosure of sensitive personal information in the support process.

We investigate our research questions in the scope of combating mobile phishing attacks. We specifically focus on two types of social support architectures: ones that rely on existing social connections and those that use community member volunteers who are anonymous to the support seeker. Our definition of successful support interactions is based on seeker and helper perceptions of reliance, learning, privacy exposure, and user satisfaction. These perceptions can be different if the helper is a close connection or from a community of volunteers. Our first research question is, what are the differences in perceptions of reliance, learning, and privacy exposure between two architectures: social networks and community of volunteers? Based on this research question, we expect the following hypotheses to hold:

- **H1** Seekers are willing to rely on close social connections more than on the community of volunteers (based on [11, 26, 28, 38, 46]).
- **H2** We assume that the notion reflected in H1 is also shared by the helpers, who would feel that their advice is more valuable to close social connections (based on [22, 25, 29]).
- **H3** Seekers will feel that they learn more from their close social connections than from the community of volunteers (based on [11, 26, 28, 38]).
- **H4** Helpers perceive high teaching from their close social connections than the community of volunteers (based on [25, 29]).

Beyond analyzing the difference between close connections and community volunteers, we characterize successful support interactions by measuring the satisfaction of both seekers and helpers and the correlation with various properties of the interaction. The second research question is what features (word count and response time) influence people's perceptions about reliance, learning, and privacy exposure in the support process. We would analyze these hypotheses while controlling for security awareness, privacy concerns, self-efficacy, and demographic properties of both seekers and helpers. Specifically, we derive a specific hypothesis from the literature:

- **H5** Seekers will feel that the helpfulness of responses positively correlates with the length of the messages (based on [26]).

3 MEERKAT

Meerkat is a mobile Android application that implements peer support for the Android operating system. The support process is visualized in Figure 1 and starts by shaking the phone to capture a screenshot (such as a suspicious phishing message), sharing with potential helpers and writing a question, selecting a helper from contacts, then receiving an answer. Our application contributes a combination of two community helpers: close connections and volunteers. The interaction model is based on a multi-model peer support process, such as the one evaluated in [26] and implemented in [26, 30], in which screenshot annotation and chat interfaces enrich user interaction through the support process.

Users can play two roles in the system: the role of a seeker (who asks for support) and the role of a helper (who provides support). The seeker can choose a helper from the community of helpers. The community of helpers refers to the users available to provide support. The seeker can be connected to the users who have social contacts (e.g., close friends, family members) or a community of volunteers who are social connections of other users who want to provide support. The support process starts when encountering an uncomfortable mobile situation, such as phishing messages, permission management, and notification from an app. The seeker starts an action that captures a screenshot, which can then be marked with questions or highlight problematic interactions on the screen.

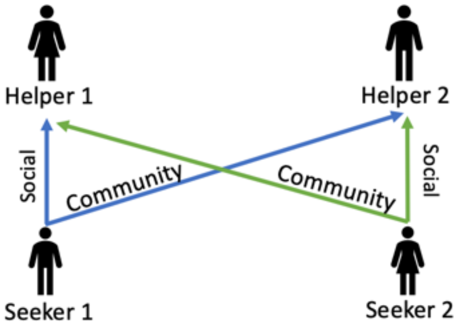


Figure 2: Users can receive support from their social connections or volunteers (social connections of other users).

The app allows users (in their role as seekers) to choose a helper by importing phone contacts (after receiving the user's consent). When the user chooses to add a contact as a helper, the contact receives a text message with a link to download the app from the Android Play Store. If the contact downloads the app, they are automatically assigned as one of the designated helpers of the inviting user. They can also volunteer as helpers to other users, supporting anonymous seekers. The app can also assign a volunteer helper to all the users who choose to receive support requests from others.

As seen in Figure 2, the same seeker can get help from their social contact helper and a community volunteer (who can be the social contact helper of another user). Seekers and helpers can annotate the screenshot with different colors to point out and highlight elements of the interaction. They can also discuss the interaction in a text message thread. If the helper is a volunteer, their name will be hidden and labeled in the chat thread only as a community volunteer.

4 METHOD

4.1 Experimental Design

The experiment was carried out in the field with participants installing the Meerkat app on their own phones. During the five-day course of the study, participants received ten tasks, each representing a phishing attempt. The manipulated variable was the helper that answered the seeker's questions, a social connection, or a community member (see Figure 2). The result is a within-subject design, where participants were randomized to different relationship types for each of the ten messages, with repeated measures for ten randomized phishing messages. We have chosen to rely on simulated phishing messages for several reasons. The main reason was to control the content of the support request and to ensure that it would not be correlated with the helper's identity. Also, we wanted to minimize privacy risks to our participants and to ask them to capture screenshots of phishing messages rather than uncontrolled screens. Finally, as the average number of phishing messages people receive is highly volatile, we could not ensure that the participants will receive enough messages through a reasonable course of the study.

4.2 Participants

We recruited paired participants by posting on the university's message boards. We stated in recruitment materials that we were looking for paired participants who live together or have strong social ties. Participants must be 18 years old and own an Android smartphone device. We verified eligibility through a short online questionnaire. We explained that the experiment required them to install an app from the Google Play store and perform ten tasks for up to five days. We offered them to select a date from four predefined dates to start the experiment.

We recruited 65 participants (32 pairs) who persisted through the whole duration of the study. One pair of participants and one individual participant assigned as the seeker withdrew in the middle of the experiment. We decided to remove all tasks related to the seeker that withdrew from the experiment but kept two tasks related to the helper whose partner withdrew to save several tasks related to the community. The total number of tasks paired participants executed together was 311 tasks and, on average, 9.7 tasks per user. The exact breakdown of tasks per participant is as follows: 20 participants completed 10 tasks, 9 completed 9, 2 completed 7 tasks, and a single participant completed 4 tasks. A handful of instances were removed from the analysis because of technical difficulties in saving the questionnaire at the end of the task.

The ages of participants ranged from 20 to 45 years, with a median of 26 years. A total of 36/65 (55%) participants identified as female, 29/65 (45%) as male, and no one of the participants chose the "prefer not to say" option. The distribution of the participants' education was bachelor's degree or above 34/65 (52%), high school 30 (46%), and one with technical school 1 (2%). Most of them reported not having a technical degree 48/65 (74%). Most of the paired participants do not live together 39/65 (60%). They declared that their relationship is friendship 34/65 (52%), siblings 12/65 (18%), married 12/65 (19%), spouse 6/65 (9%), and engagement 2/65 (3%).

4.3 Participants Assignment

In this study, we configured the Meerkat app for the experiment. First, we randomly assigned a participant to a role, seeker or helper, when adding the participants to the system. We manually added participants to the app to make sure that they were randomly assigned to roles. Second, participants who were randomly assigned to the seeker role received tasks through the Meerkat app, and we asked them to request support from the helper (see the process in Figure 1). Finally, we randomly assigned the social contact helper or a community volunteer, i.e., the seeker sent five support requests to the social contact and five messages to the community member (see in Figure 1 B the bold text "family member or a close friend", otherwise the app will display "community member"). The seeker can see the helper's name only when the app randomizes the social contact helper. Otherwise, the seeker sees a "community member" (Figure 1 E).

4.4 Procedure

After paired participants registered for the study, we sent them an email confirming their participation. Before the experiment started to date, we randomly assigned each participant paired to a role: one was randomized as a seeker, and the other one was to be a helper. Then, we randomly assigned each seeker to another helper, as can be seen in Figure 2. It represents two seekers, two community members, and two social support helpers. The study included three main steps: onboarding, task support interaction, and a final questionnaire. The exact questionnaire, translated from the original Hebrew, is fully described in Appendix A.2. Each step included the following:

Onboarding. Participants digitally signed a consent form informing them about the experiment, describing the collected data, and how the data was going to be used (more about the consent form section 4.6). Participants received an explanation of the experimental procedure and were asked to install Meerkat from the Google Play store and perform ten tasks for up to five days. Then, the participants reported their demographics: gender, year of birth, education degree, technical background, and relationship with the paired user (friends, intimate relationship, etc.), whether their paired participants are living in the same house, privacy concerns questionnaire, security awareness questionnaire, and digital literacy questionnaire. After the questionnaire, they installed the app using the attached link to the Google Play store.

Task procedure. The application alerted the seeker participants using a notification when a new task was ready. Each task included a simulated text phishing message. The system presented the seekers with ten phishing messages over four days. The seeker sent five support requests to their paired participant for social support and five support requests to the community member, a randomized helper. The application randomly decided which was the designated helper, and the seeker was informed about the type of helper. In total, each participant executed ten tasks on average. To complete a task successfully, the participants should apply the following steps:

1. The seeker receives a new task in the tasks tab (see Figure 1 A), followed by a notification. To make sure that our participants did not miss a notification, we guided participants to check the application every several hours to observe whether they received messages. Participants who did not open their notifications were reminded to do so through email or other forms of communication.
2. When the seeker enters the task, we show an explanation about the task (Figure 1 B): "Meerkat will show you a text message. Please imagine that this is a text message sent to your device. Use the 'take a screenshot' button to send a support request to a <relationship type>." The app randomized the relationship type to either "family member or a close friend" or "community member".
3. The seeker receives a screenshot of the text message and is requested to ask the helper whether this text message is safe (Figure 1 C). The seeker writes a support request, including

a screenshot with a drawing using a yellow marker, a red pen, or a black brush to hide private information (see Figure 1 D).

4. The seeker sends the request to the helper that was randomized by the application.
5. The helper receives a notification and can see the messages under the "Support" tab. The helper can write back a short explanation and draw on the same screenshot the seeker sent, which is useful when the helper and the seeker may have different operating systems.
6. The seeker receives the helper response on the "my issues" tab. The seekers are required to enter and read the message (see Figure 1 F). The seeker and helper can keep communicating through the chat thread.
7. The helper and the seeker receive a short post-task questionnaire about the task. The questions are displayed in Table 1.
8. The app randomizes the timing of the next task and sends another task. After ten tasks, the application will send an exit questionnaire to the paired participants.

Exit questionnaire. Finally, participants filled out an individual exit questionnaire describing the experience of receiving and providing support using the app with close social connections and a community of volunteers.

4.5 Phishing Messages

We collected most phishing messages from real-life phishing attacks and followed a similar structure: starting with the sender's name, a short text message, and ending with a URL link. For example, "We recognized a new login into your account from a new device you have not logged in to before. We sent you this message to verify that it was not someone else. Login into the activity right now www.google.abc135.com/google121121." The full text of the phishing messages is available in Appendix A.3.

We have guided the seeker to ask for support on how they can analyze the message and infer whether it is safe or not. The ten text messages contain spoofed URLs that the helper expected to identify and warn the seeker not to click on the link. The spoofed URLs make users believe clicking on them will open the genuine site. URL confusion stems from a misunderstanding of URL parsing [12]. We have two spoofed URL types in the experiment: six URLs that contain a sub-domain with the sender's name, and the four do not include a sub-domain related to the sender's name.

4.6 Ethical Considerations

As our study involved a field study that mediates communications between participants and the collection of personal information, we have made several ethical considerations about our method. First, our field study was reviewed and approved by our institutional ethics review board. The board approved the objectives of the study, the method, the questions that participants were asked, the information we collected, and the consent form that the participants agreed to. Potential participants were asked to review and agree to a consent form (the full form is available in Appendix A.1). We gave special consideration to etiquette and respectful behavior between participants, as they will be in contact with others that they do not already know. Therefore, we have created and notified participants regarding our policy for mutual respect, expected behavior, and mutual privacy. We provided ways for participants to contact the research staff to enforce it.

To minimize the potential harm to participants from sending screenshots of their phones, we have based our study on the prompted phishing messages, so the screenshots do not contain personality identification information. Furthermore, the seeker and the helper sent text messages. This experiment design does not expose the participants to any security risk because it's a hypothetical scenario in a controlled application. We asked the participants not to write personality identification information and, if they wrote it, to inform the researchers immediately to delete it. We did not receive any complaints about the information disclosure concerns in the text messages and, in general, during and after the study. The data was encrypted during transit using HTTPS, and it was stored in a logically isolated database. Participants could exercise their rights to data access and deletion by contacting the research staff through email or phone.

The communication between the seeker and the community member was anonymized. We kept the community member identity hidden by displaying only "community member". We also asked participants not to reveal their identity to other participants that they did not know beforehand. In the experiment version app, we registered the paired participants together and labeled them as social contact or volunteers. Only social contact connections could see each other nicknames in the support interactions. Finally, participants were reimbursed in the equivalent amount of $25 US dollars for participating in the study.

4.7 Variables

We have collected information about the interaction between the seeker and helper for each task. The individuals reported privacy concerns, security awareness, digital literacy, and demographics. Privacy concerns measure individuals' perceptions about sharing personal information with applications, the items from the organizational information privacy practices instrument [43]. Security awareness captures security behavior intentions and actual security behavior. The items were adopted from the proactive awareness subscale group [14]. Digital literacy measures familiarity with technology and smartphone uses hours [15, 16]. We asked participants if they were familiar with internet-related items and asked for several demographic characteristics.

The interaction between helper and seeker is collected for each task. Within the condition is the source type that defines whether the helper is a contact or a community member. The objective measures are the number of words in the helper message, the number of words in the seeker message, and the time the helper responds in hours for each task.

Table 1 presents the variables for the helper and seeker for each task: the answers to five subjective questions related to the seeker's perceptions after each task and five subjective questions related to the helper's perceptions after each task. The seeker's reliance is related to the seeker's willingness to accept the helper's advice. Helper's perceived reliance represents the belief that the seeker will adopt the recommendation. Perceived learning measures the

Table 1: The question items (variables) that were asked of seekers and helpers in the post-task questionnaire

Variable	Features	Reporting
Reliance	Would you perform the instructions in the response you received from <relationship type> if the message was displayed on your device? Yes, I will do it. No, I won't do it. I don't know	Seeker
Learning	The support response I received from <relationship type> helped me learn how to perform the task	Seeker
Exposure	It bothers me that <relationship type> was exposed to sensitive information during the support	Seeker
Text Satisfaction	The text I received from <relationship type> successfully explained the problem I encountered	Seeker
Drawings Satisfaction	The drawings I received from <relationship type> helped me to understand how to perform the task	Seeker
Perceived Reliance	Do you think your answer will be performed on the mobile device of <relationship type> who asked for help? Yes, it will be done. No, it won't be done. I don't know.	Helper
Perceived Teaching	I think that my response allowed <relationship type> to learn how to perform the task	Helper
Perceived Exposure	I was exposed to sensitive information related to <relationship type> during support	Helper
Helper Text Satisfaction	The text written by <relationship type> successfully described the problem	Helper
Helper Snapshot Satisfaction	The screenshot sent by <relationship type> helped me understand the text	Helper

seeker's subjective learning from the support. The perceived teaching measures the helper's opinion that succeeds in teaching the seeker how to perform the task. The received text, snapshot, and drawings satisfaction measure how the design features help interact with the helper and seeker. The exposure measures the users' concern with the disclosure of sensitive personal information while requesting and providing support and influence the willingness to ask and provide support.

4.8 Analysis

Our quantitative analyses were based on mixed effects models because of our repeated measure experimental design in which the same user performed several tasks. We used Generalized Linear Mixed Effects models to create two models: one for the seeker's reliance and another for the helper's reliance (with the participant ID and task ID as random effects). We also used Ordinal Mixed Model regression, which uses the perceived learning, exposure, messages text, and drawings satisfaction as the dependent variables (with the participant ID and task ID as the random effect variables). We collected qualitative data to understand users' preferences about receiving and providing social support. At the end of the study, we asked participants several closed and open-ended questions about their preferences. We have categorized the answers with an iterative thematic analysis. The responses were read iteratively by the first author to initially code the data to find similarities and differences across participants. We explored the data for categories and central themes through frequent meetings with a second researcher.

5 RESULTS

5.1 Reliance

To characterize the extent to which users felt that they could rely on others advise, we created two generalized linear mixed-effects models: one for the seeker's reliance and another model for the helper's perceived reliance. Figure 3 shows that the seeker's reliance was higher by 8% for receiving help from close connections than community volunteers support (AIC= 272.97, BIC = 284.19, $p<0.05$). We found similar results in the perception of helpers, and whose perceived reliance was higher by 12% in helping close connections than community seekers (AIC= 256.73, BIC = 267.95, $p<0.0001$). In the helper's perceived reliance, the proportion of unknown cases increases from 10% in close connections to 22% in the community. While in the seeker's reliance, the proportion of unknown cases increases only from 7% in close connections to 10% in the community. The results indicate that helpers may have more difficulty understanding if the community seekers rely on them than close connection seekers.

5.2 Seekers' Perspectives

To understand the important factors in determining the experience of seekers in Meerkat, we created a model that included both task variables and personal variables: we investigated the learning perceptions, privacy exposure, and satisfaction with relationship type, word count, time response, and the seeker's demographic variables. Table 2 presents ordinal mixed model regression to characterize the effect of multiple properties on the seeker's perceived learning (AIC= 631.50, pseudo-R^2=14.5%), perceived exposure (AIC=649.12, pseudo-R^2=29.3%), the satisfaction of received text (AIC=475.39, pseudo-R^2=23.5%), the satisfaction of drawings received (AIC=592.70, pseudo-R^2=23.5%). The gender variable in the analyses contained only males and females since no one from the participants did not choose a different option. We found that in 84% of the support interaction, the seekers agreed and strongly agreed they learned from the support interactions. Yet, Figure 4 shows that seekers' learning from close connections is 8% higher than community volunteers' support (coefficient of 0.388, $p<0.001$). This is also true for exposure. The seeker exposure information

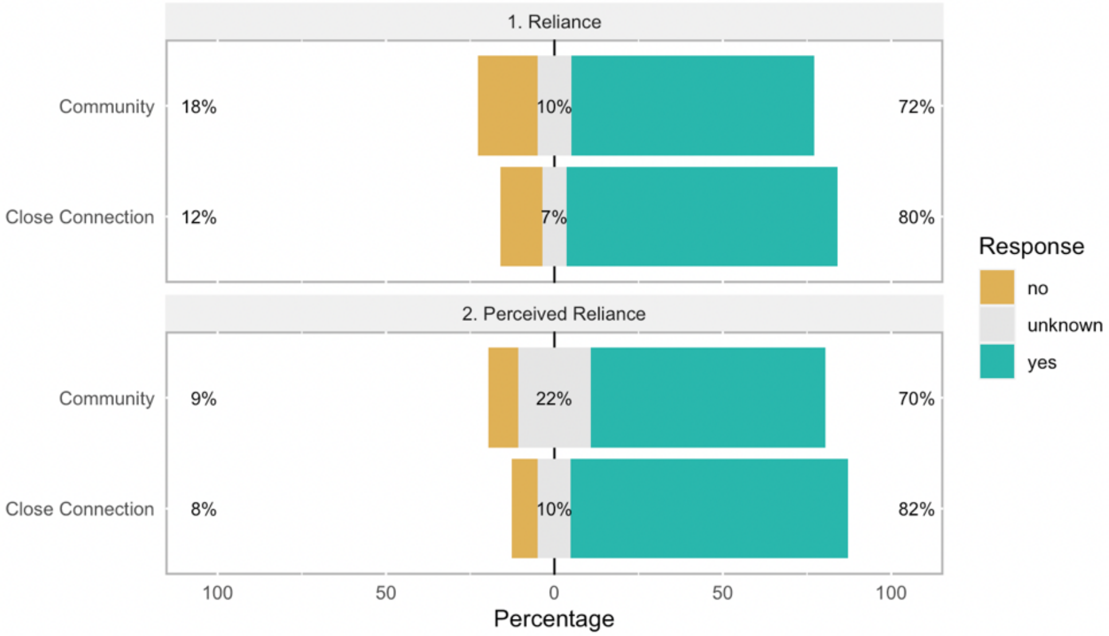


Figure 3: The seekers’ reliance and helpers’ perceived reliance are grouped by the relationship type (community member and close connection).

Table 2: Ordinal mixed model regression for seekers’ perceived learning, perceived exposure, text received satisfaction, and drawing received satisfaction. Each cell contains estimates, and significance levels are noted by: p < 0.0001’ *’; p < 0.001’**’; p < 0.05’*’.**

	Seeker							
	Learning		Exposure		Text Satisfaction		Drawings Satisfaction	
Property	β	p	β	p	β	p	β	p
Seeker Age	0.020		-0.158	*	0.029		0.054	
Seeker Gender: Male	0.090		-0.119		0.113		0.534	
Seeker Tech Degree: Yes	-0.134		-0.069		0.130		0.496	
Seeker Mobile Hours Use	-0.003		0.007		-0.047		0.037	
Seeker Privacy Concerns	0.319		-0.272		0.448		0.145	
Seeker Digital Literacy	0.288		0.678		0.438		0.246	
Helper Security Awareness	-0.069		-0.419	*	-0.063		0.269	
Seeker Security Awareness	-0.623	*	0.591		-0.366		-0.730	**
Helper words count	0.023	*	0.004		0.058	***	0.012	
Seeker words count	0.002		-0.016		-0.013		-0.008	
Time Helper Responses	0.019		-0.022		0.016		-0.011	
Relationship type: Social	0.388	**	-0.874	***	0.187		0.215	

from close connections is 17% lower than the community member’s support (coefficient of -0.874, p<0.0001). Seekers also felt more exposed when sharing screenshots with community members. However, the relationship type was an insignificant factor in the text and drawings satisfaction received from the helper. The seekers believed that most of the messages successfully from the helpers explained the problem (93% of the text messages were ranked as agreed or strongly agreed with the text satisfaction).

To understand the factors that point out a good support interaction, we have analyzed several correlations between quality measures such as learning and satisfaction and properties of the interactions. These relationships are visualized in Figure 5. The number of words that the helper sent to the seeker is positively correlated with positive learning perceptions (coefficient of 0.023, p<0.05) and with the satisfaction with the text (coefficient of 0.058, p<0.0001). The awareness of both seekers and helpers to security was also

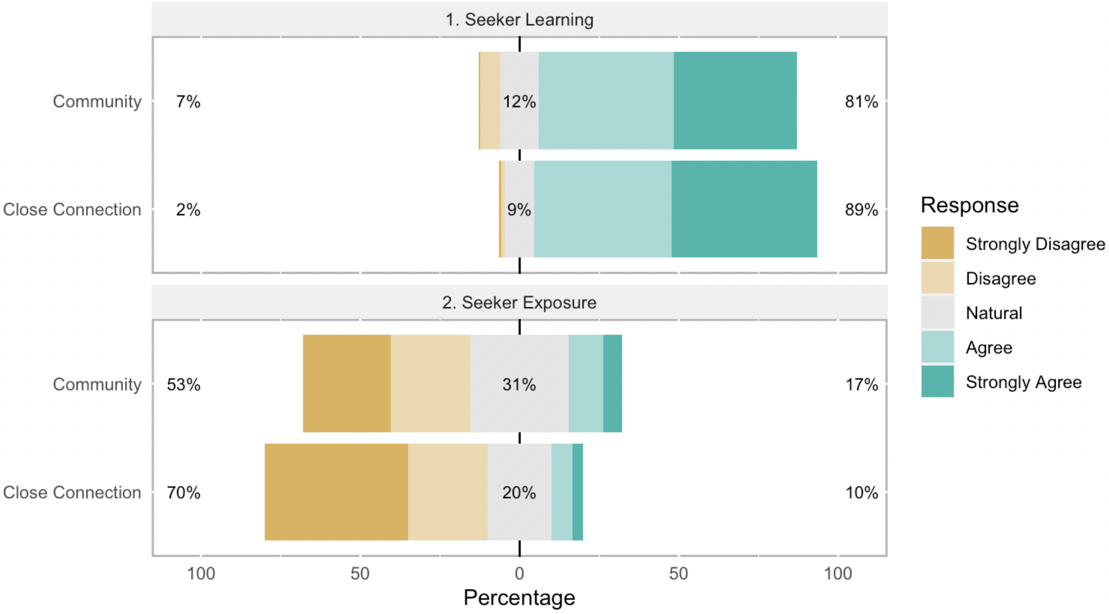


Figure 4: Seeker-perceived learning and seeker-perceived exposure are grouped by the relationship type (community member and close connection).

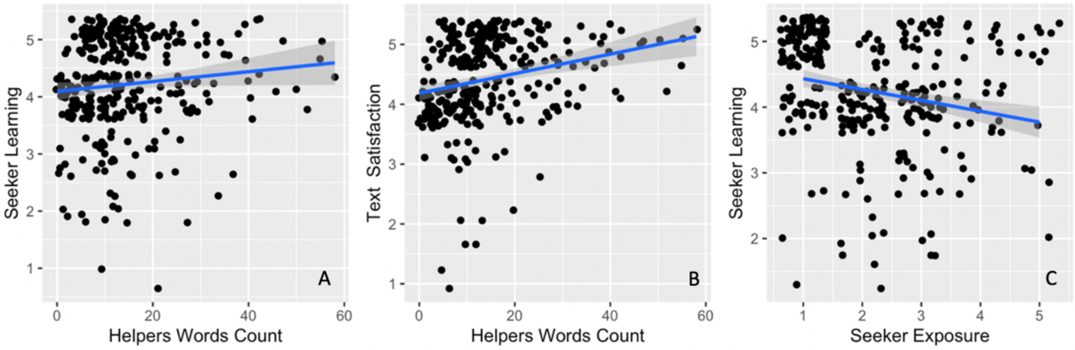


Figure 5: (A) The relationship between the seeker's perceived learning and the number of words in the helper response. (B) The relationship between the seeker received satisfaction and the number of words in the helper response. (C) The relationship between the seeker's privacy exposure and learning.

meaningful in our model. The seeker's security awareness is negatively correlated with learning perceptions (coefficient of -0.623, $p<0.05$) and drawing satisfaction (coefficient of -0.73, $p<0.05$). The helper's security awareness is negatively related to information exposure (coefficient of -0.419, $p<0.05$). Demographic variables played a limited role in our model. With regard to demographics, we did not find a significant relationship with gender. Age was negatively correlated with information exposure from social connections (coefficient of -0.155, $p<0.05$).

Our findings point to the complexities of the seekers' privacy concerns. Providing relevant help without compromising privacy is not a straightforward process, and our findings point to an inherent difficulty in peer support and to some negative externalities. As Figure 5 shows, there is a negative correlation between seeker privacy exposure and learning (spearman correlation test, r=-0.33). Seekers feel that they learn less from interactions in which they feel more exposed. This finding provides an additional explanation for the higher levels of perceived learning from the interaction with social connections, as they pose less of a privacy threat to users. It also points to the importance of protecting the seekers' privacy, as it may be the key to sharing enough information that may lead to meaningful learning.

5.3 Helpers' Perspectives

We explored how the helpers' perceptions, awareness, and satisfaction are related to the relationship type, word count, time response,

Table 3: Ordinal mixed model regression for helpers' perceived teaching, perceived exposure, text received satisfaction, and drawing received satisfaction. Each cell contains estimates, and significance levels are noted by: p < 0.0001' *'; p < 0.001'**'; p < 0.05'*'.**

	Helper							
	Teaching		Exposure		Text Satisfaction		Snapshot Satisfaction	
Property	β	p	β	p	β	p	β	p
Helper Age	-0.024		-0.052		0.028		0.067	
Helper Gender: Male	-0.189		0.447		-0.369		-0.969	
Helper Tech Degree: Yes	-0.556		-0.899		0.076		-0.445	
Helper Mobile Hours Use	-0.114		-0.077		-0.059		-0.019	
Helper Privacy Concerns	-0.138		1.079	**	-0.242		-0.377	
Helper Tech literacy	0.241		-0.015		-0.151		-0.101	
Helper Security Awareness	1.072	*	-0.341		0.712		0.889	*
Seeker Security Awareness	0.225		-0.093		-0.052		-0.013	
Helper words count	0.013		-0.007		0.004		0.021	
Seeker words count	-0.012		-0.003		0.022		0.014	
Time Helper Responses	-0.002		0.040		-0.014		-0.042	
Relationship type: Social	0.290	*	0.132		0.629	***	0.419	

and the seeker's demographic variables. Table 3 presents the results of the ordinal mixed model regression to characterize the effect of multiple properties on perceived learning (AIC= 581.55, pseudo-R^2=25.4%), perceived exposure (AIC=602.19, pseudo-R^2=29.5%), the satisfaction of received text (AIC=568.16, pseudo-R^2=23.7%), satisfaction of the received snapshot (AIC=475.97, pseudo-R2=26.6%). While 77% of the support interaction agreed and strongly agreed they taught the seeker through the support interactions, close connections have a 13% higher effect than community support on helpers' teaching beliefs. as displayed in Figure 6 (coefficient of 0.295, p<0.05). Furthermore, the text written by social connections has successfully described the problem at 8% higher than a community volunteer (coefficient of 0.629, p<0.0001), and the snapshot from the close connection is 6% higher in explaining the problem than the snapshot from a community volunteer (coefficient of 0.419, p<0.05). Overall, we can say that when helpers and seekers have a social connection, the helper better understands the seeker's questions and the digital security situation.

The helper's security awareness is correlated with several important aspects of providing support. As visualized in Figure 7, when helpers have higher security awareness, they believe that they also provided more meaningful support to the seeker (coefficient of 1.072, p<0.05). They also have higher satisfaction in the seeker' snapshots (coefficient of 0.888, p<0.05). A possible interpretation is that people with higher security awareness may believe they can teach the seeker and are interested in receiving a snapshot to understand the situation better to provide support. Finally, when helpers' have deeper privacy concerns, they feel that they are more exposed to seekers' private information (coefficient of 1.955, p<0.05).

5.4 Users' Support Preferences

To understand users' preferences about receiving and providing social support, we asked seekers at the end of the study several closed and open-ended questions about their preferences. We directly asked about whom they prefer to request and helpers who would like to provide support through the app. Figure 8 shows that seekers have a strong preference to receive support from a close connection (65%) than from both a community volunteer and a close connection (25%). On the other hand, helpers' preferences were not as strong: they preferred to provide support to close ties and community seekers on roughly equal terms (55%). As seeker and helper roles were randomly assigned at the beginning of the study, we can assume that the differences resulted from their five-day experience.

Using an open-ended question format, we asked participants to explain their preferences. We have categorized the answers with an iterative thematic analysis. A common explanation by seekers is privacy concerns about disclosing personal information to a close relationship rather than to a community member (6 out of 32). For example, one participant reported, "I feel more comfortable disclosing personal information to a relative than a community member whom I don't know," which was also observed in the seeker's exposure. Seekers also said they were more comfortable asking questions close connections than community volunteers (5 out of 32), for example, "It's easier to ask a question from someone I know than someone I don't know." This was also observed in our model when the helper's satisfaction with the text written by social connections successfully described the problem more than community members. Two people mentioned the quality of the helper's answers. For instance, "the relative gave me more detailed information, but the community member gave shorter answers, a little less detailed." This was also observed through the number of words that were provided in the help response by the helper.

Seekers also mentioned trust as an essential factor (5 out of 32). For example, "It is easier to consult such a person <a close connection> and to trust him". Seekers described a tradeoff between social closeness and the expertise of the helper (5 out of 32). For example, "community members have more extensive knowledge about certain things. Still, there are times when it's more personal or sensitive information that I wouldn't necessarily want to reveal

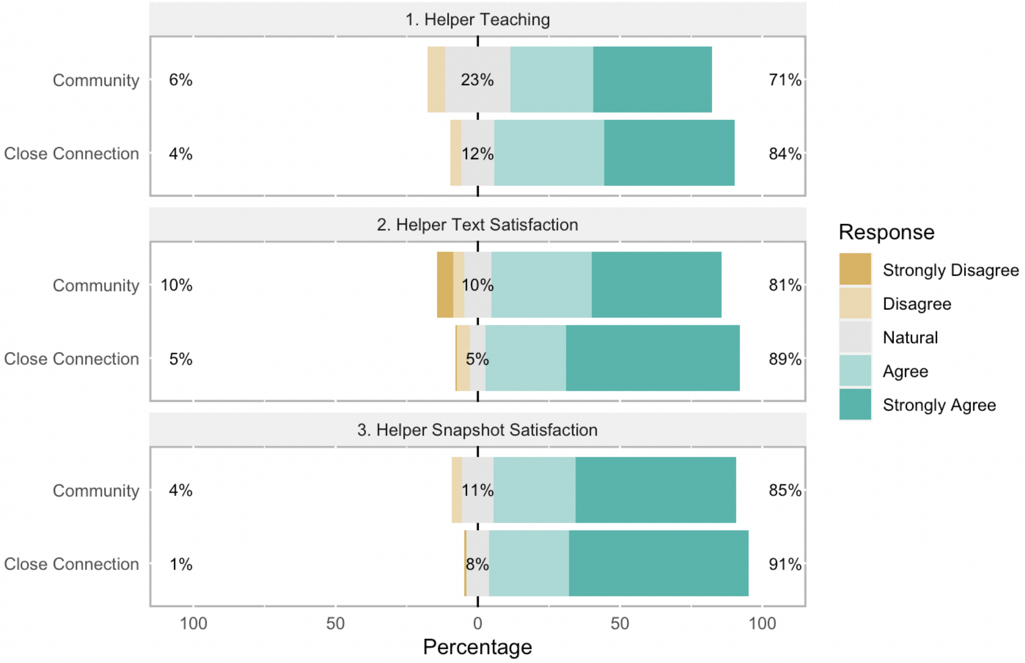


Figure 6: Helper-perceived teaching, helpers' text satisfaction, and helpers' snapshot satisfaction were grouped by the relationship type (community member and close connection).

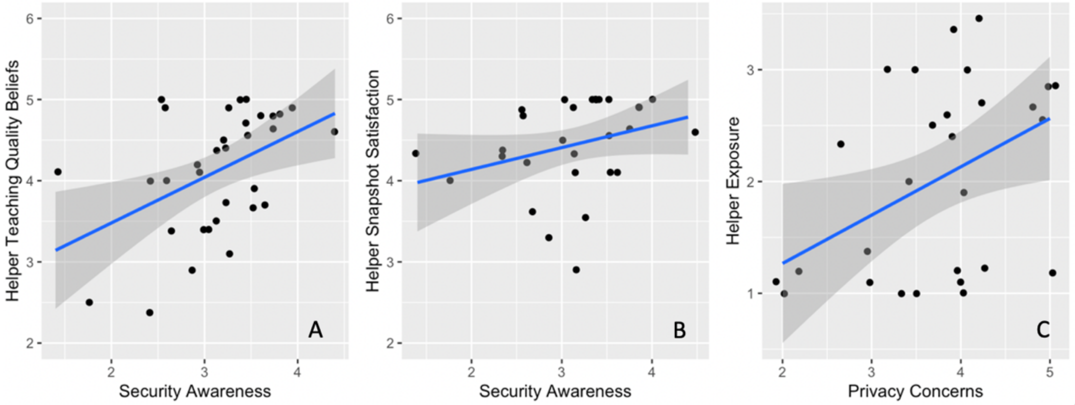


Figure 7: (A) The relationship between the helper's quality of teaching and security awareness. (B) The relationship between the helper snapshot received satisfaction and security awareness. (C) The relationship between the helper's exposure satisfaction and privacy concerns.

to outsiders." Another participant mentioned, "It would be nice for someone close to you to respond, especially if it is about personal details, although I would prefer someone who knows what it is about instead of a close friend." We should mention that in the experiment communities' volunteers do not have necessary higher expertise than social connections. However, future design may consider ranking community members based on their expertise and compare between volunteers and social connections. So, the volunteers will have higher expertise than the social connection.

Seven helpers felt more comfortable supporting close ties because they care about their daily problems. One helper reported that he did not feel comfortable sending disclosure messages: "sending of screenshots and the disclosure of messages I receive, I don't necessarily feel comfortable sending it to someone I don't know." Another helper described the richer interaction with his friend, who asked more extended questions with more details: "The friend asked me for more extensive information and provided detailed the small things."

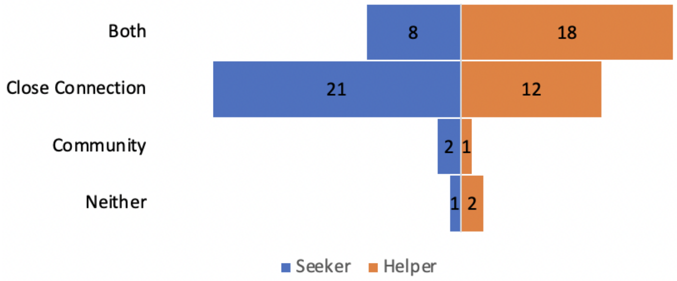


Figure 8: Distribution of relationship type preferences for seeker and helper

6 DISCUSSION

6.1 Experiential Findings

We conducted a field experiment that compared support from close connections and community volunteers providing support related to phishing messages. Our findings point to the importance of this basic design choice in social support systems. To analyze the support differences between close connections and community volunteers, we needed to combine several measures that were used in the past only independently (as in [46]). These include the reliance on the given advice, how much users learned from the interaction, how exposed they felt when sending screenshots, and what is their satisfaction with various aspects of the interaction.

As the literature teaches us, security support relationships can be richer than we might think. It can allow the helper to provide a wide array of support interactions, including advising, guiding, demonstrating, or fixing the problem on behalf of the seeker [29]. However, not every support interaction is equally useful, and not all of them result in higher self-efficacy for the seekers. Our findings point to the effectiveness of using multi-modalities in the support process. Seekers reported high levels of learning and reliance on support, with positive indicators above 70% for both types of relationship type. In both types of interactions, our participants reported 70%-80% willingness to act on the suggestion of the helper. Previous studies have shown that support processes that are limited to fixing the technical problem do help users regain knowledge and confidence in facing those challenges independently in the future [18, 46]. Moreover, helpers reported high levels of satisfaction with their answers and the quality of their responses, again for both relationship types.

Our findings show that users tend to rely on and learn more from the advice of their close connections compared to community volunteers. The difference between close connections and community volunteers was evident in most of our dependent measures, and the effect ranges around 10% lift for close connections. This moderate difference may point out that in technical support, social relationship plays a smaller part than in other forms of social security behavior (such as in [28].) The differences can be attributed, at least in part, to the better understanding the helper has of the seeker and their preferences, as previously reported in qualitative observations [26]. The reliance can be attributed to the higher trust they have in their connection, which they might not have with an anonymous community helper. The fact that both reliance and learning were higher for close connections may point to the contribution of the knowledge helpers may have about their closer connection being meaningful to provide high-quality support. Privacy was a major concern for our seekers and helpers, and here too, the connection type had a significant effect. Our participants cited privacy as one of the major reasons for choosing close connections rather than community members. Similarly, seekers were more concerned about exposing their screenshots to strangers than community members. This points to the importance of privacy management solutions when sharing information in rich support environments.

The correlation between the satisfaction and the length of the corresponding points to the importance of encouraging discussions between the seeker and helper. The previous study has shown the importance of conversations among close social members, which encourages them to adopt security behaviors when discussing security features [11]. These results are encouraging and demonstrate the potential of social support systems. However, there are meaningful differences between the way users perceive and apply meaning to the interactions.

To corroborate these self-reported measures, we have compared them with the characteristics of the actual interaction. These comparisons allowed us to gain confidence in the measures and their meaning. For example, we see that the number of words written as a response by the helper is highly correlated with the satisfaction of the seeker from the text (but not with the satisfaction from the marked screenshot). This characterization can contribute to successful support interactions. Seekers were less likely to learn from the helpers' input if their security awareness was higher and, overall, were less satisfied with the markings on their screenshots (even when controlling for the connection type). Helpers with higher security awareness perceived their own advice as more satisfying.

6.2 Design of Community-based Support Systems

In a rich support environment, such as in Meerkat, the relationships between the seeker and the helper become crucial to the performance of the support process. Meerkat's design aims to enhance social support to allow users to leverage their personal and collective resources to address mobile security and privacy challenges. It aims to provide a richer set of supportive relationships, which also allow helpers to guide and advise the seeker. The design of Meerkat is based on a shared space in which seekers and helpers can communicate over the support process, using captured screenshots, marking these screenshots, and a chat thread that can embed the screenshots.

Our findings point to several ways support systems can be better designed. We argue that both social-based systems and community-based systems can be used, but they can be used in different ways and in different contexts. Close connections seem to solve several tough support problems, at least partially. They provide more informed support in a more comfortable environment. But naturally, they may come with an increased burden on helpers. We also observed a tradeoff between closeness and the expertise of the helper. This type of tradeoff can be used as a design roadmap, focusing on one type of support if the conditions seem to favor it; for example, in situations that do not have sensitive information, community-based architectures might be more suitable. Alternatively, we can imagine systems that delegate support to the most appropriate helper while considering how sensitive the information is, how important expertise is, and other factors.

Making community volunteers feel closer than they really are another interesting approach. A possible design implication is adding endorsement and recommendation [17]. Adding cues, creditability, or popularity rating as a form of endorsement may help seekers rely on and learn from the community member. Another possible implication for design is to guide or nudge helpers to write long messages to allow the seeker to understand the support. It can be helpful to guide the helper to write longer explanations, and meaningful explanations can improve learning as exposure to personal information may affect the helper's motivation to provide support [29]. Thereby it is essential to protect the seeker's private information during the support process. It can be very useful to explore mechanisms recognizing when private information is shared with the community to avoid seekers experiencing regrets about online disclosures in the support process. Wang et al. investigated mechanisms based on soft paternalism that identified and nudged users to explore the message before posting on social media [47]. Future studies can examine these nudge mechanisms in the support process. While our findings were collected in the context of security social support, they might also be relevant to other types of support or to other domains that may benefit from collective action and interaction, such as countering misinformation online or increasing urban safety.

6.3 Limitations and Future Work

We would like to highlight several aspects of our work that can be relevant to its external and ecological validity. First, our sample was skewed toward younger technology users, resulting from a sampling bias in recruiting college-aged participants. Future research with more varied populations could help understand the influence of demographic properties and technical expertise on the factors we studied. As many of the current literary works in collective efficacy are focused on older adults (see [46], for example), it may be interesting to see which of our findings can be replicated with a more diverse population. Second, we explicitly recruited pairs who knew one another. One limitation of this design choice is that each group in our study may not represent the more complicated social relations in larger communities. Yet, this sampling method was intentionally chosen because we wanted to understand the long-term dynamics between close connections. The way participants had indicated their gender is another limitation of our study. Our design offered only three options to participants: male, female, and prefer not to say. This questionnaire design might prevent participants from expressing their gender in an individual way, and especially non-binary identities [44].

Our analysis was based on predefined phishing messages rather than on security and privacy questions the participants might independently choose through the study. This experimental design choice was made to make sure that random effects were standardized throughout the study, between participants, and between interactions. It also had some practical reasons: to limit the exposure of personal content from the phones of the participants and to make sure there would be enough security interactions throughout the study (given the fact that the probability of each individual participant receiving a phishing email or text message during the time of the study is rather low). We have also used realistic phishing messages and followed well-known protocols [34].

We highlight several directions for future research. First, our measurement of support quality was based on subjective measurements. We were not able to analyze the actual support due to privacy constraints. Analyzing the content of the support text and interactions in a privacy-preserving way can teach us more about the interaction between helper relationships and expertise. While the source code for Meerkat cannot be opened at this point, the application itself can be downloaded and experienced. From the engineering standpoint, future studies can develop allocation mechanisms that optimally assign community volunteers and social connections for support tasks. Another aspect that was not addressed in this paper is how to make sure peer-support systems are safe and effective for users. These research questions span from making sure no bad faith actors use the support systems to scam or harm other users and addressing questions of support quality through creditability metrics and rating systems [29]. It is also important to recognize that Meerkat, in its current form, is a reactive system in which users need to be active when seeking support. Proactive approaches for support, such as the ones suggested in [27], can also affect how users interact with both social connections and community volunteers.

7 CONCLUSION

We present a design and an experimental evaluation of Meerkat, an application that uses both community members and existing social connections for collective support. We investigated how seekers and helpers interacted when receiving support in online security from family or community volunteers. We conducted an experiment that uses Meerkat, which helps seekers to tackle hurdles in interacting with mobile applications by receiving contextual support from friends and family or community volunteers. Our results show that close connections have higher perceived learning and reliance on online security than the community of volunteers. Users' perceived learning is significantly correlated with the number of words the helper writes in the support text messages. We also qualitatively analyze seekers' preferences to receive support to understand their preferences and the reasons behind them. We found that seekers prefer to receive support from close connections because they feel comfortable disclosing personal information, asking questions, trust and quality of the advice. Most people consider community members when they are interested in receiving from an expert. We conclude the paper by discussing how our findings can be used to design community-based applications with different sources between helpers and seekers.

ACKNOWLEDGMENTS

This work was supported by the ICRC – Blavatnik Interdisciplinary Cyber Research Center, grant number 144. We would also like to thank David Lo, Debin Gao, Eran Tromer, and Shahar Maoz for their advice and feedback.

REFERENCES

[1] Zaina Aljallad, Wentao Guo, Chhaya Chouhan, Christy Laperriere, Jess Kropczynski, Pamela Wisnewski, and Heather Lipford. 2019. Designing a Mobile Application to Support Social Processes for Privacy Decisions. February: 1–12. https://doi.org/10.14722/usec.2019.23016

[2] A Bandura. 1982. Self-efficacy mechanism in human agency. Amer Psych 37, 2: 122–147.

[3] Albert Bandura. 1977. Self-efficacy: Toward a unifying theory of behavioral change. Psychological Review 84, 191–215. https://doi.org/10.1037/0033-295X.84.2.191

[4] Albert Bandura. 1997. Self-efficacy: The Exercise of Control.

[5] Albert Bandura. 2000. Exercise of Human Agency Through Collective Efficacy. 75–78.

[6] Abdul Basit, Maham Zafar, Xuan Liu, Abdul Rehman Javed, Zunera Jalil, and Kashif Kifayat. 2021. A comprehensive survey of AI-enabled phishing attacks detection techniques. Telecommunication Systems 76, 1: 139–154. https://doi.org/10.1007/s11235-020-00733-2

[7] Annie T. Chen, Shaoqing Ge, Susie Cho, Andrew K. Teng, Frances Chu, George Demiris, and Oleg Zaslavsky. 2021. Reactions to COVID-19, information and technology use, and social connectedness among older adults with pre-frailty and frailty. Geriatric Nursing 42, 1: 188–195. https://doi.org/10.1016/j.gerinurse.2020.08.001

[8] Chhaya Chouhan, Christy M. Laperriere, Zaina Aljallad, Jess Kropczynski, Heather Lipford, and Pamela J. Wisniewski. 2019. Co-designing for community oversight: Helping people make privacy and security decisions together. Proceedings of the ACM on Human-Computer Interaction 3, CSCW. https://doi.org/10.1145/3359248

[9] Doron Cohen, Or Naim, Eran Toch, and Irad Ben-Gal. 2021. Website categorization via design attribute learning. Computers and Security 107: 102312. https://doi.org/10.1016/j.cose.2021.102312

[10] David Constant, Lee Sproull, and Sara Kiesler. 1996. The Kindness of Strangers: The Usefulness of Electronic Weak Ties for Technical Advice. Organization Science 7, 2: 119–135. https://doi.org/10.1287/orsc.7.2.119

[11] Sauvik Das, Tiffany Hyun-Jin Kim, Laura A Dabbish, and Jason I Hong. 2014. The Effect of Social Influence on Security Sensitivity. SOUPS '14: Proceedings of the Tenth Symposium On Usable Privacy and Security: 143–157. https://doi.org/10.1145/2660267.2660271

[12] Giuseppe Desolda, Lauren S. Ferro, Andrea Marrella, Tiziana Catarci, and Maria Francesca Costabile. 2022. Human Factors in Phishing Attacks: A Systematic Literature Review. ACM Computing Surveys 54, 8. https://doi.org/10.1145/3469886

[13] Rodrigo Mariano Díaz. 2020. Cybersecurity in the time of COVID-19 and the transition to cyberimmunity. Facilitation of Tansport and Trade in Latin America and the Caribbeanand, 6: 17. Retrieved from https://www.cfr.org/blog/cybersecurity-time-covid-19

[14] Serge Egelman and Eyal Peer. 2015. Scaling the security wall: Developing a security behavior intentions scale (SeBIS). Conference on Human Factors in Computing Systems - Proceedings 2015-April: 2873–2882. https://doi.org/10.1145/2702123.2702249

[15] Eszter Hargittai. 2005. Survey measures of web-oriented digital literacy. Social Science Computer Review 23, 3: 371–379. https://doi.org/10.1177/0894439305275911

[16] Eszter Hargittai and Yuli Patrick Hsieh. 2012. Succinct Survey Measures of Web-Use Skills. Social Science Computer Review 30, 1: 95–107. https://doi.org/10.1177/0894439310397146

[17] Brian Hilligoss and Soo Young Rieh. 2008. Developing a unifying framework of credibility assessment: Construct, heuristics, and interaction in context. Information Processing and Management 44, 4: 1467–1484. https://doi.org/10.1016/j.ipm.2007.10.001

[18] Amanda Hunsaker, Minh Hao Nguyen, Jaelle Fuchs, Gökçe Karaoglu, Teodora Djukaric, and Eszter Hargittai. 2020. Unsung helpers: older adults as a source of digital media support for their peers. Communication Review 23, 4: 309–330. https://doi.org/10.1080/10714421.2020.1829307

[19] Ankit Kumar Jain and B. B. Gupta. 2022. A survey of phishing attack techniques, defence mechanisms and open research challenges. Enterprise Information Systems 16, 527–565. https://doi.org/10.1080/17517575.2021.1896786

[20] Jess Kropczynski, Zaina Aljallad, Nathan Jeffrey Elrod, Heather Lipford, and Pamela J Wisniewski. 2021. Towards Building Community Collective Efficacy for Managing Digital Privacy and Security within Older Adult Communities. Proceedings of the ACM on Human-Computer Interaction 4, CSCW3: 1–27. https://doi.org/10.1145/3432954

[21] Jess Kropczynski, Reza Ghaiumy Anaraky, Mamtaj Akter, Amy J. Godfrey, Heather Lipford, and Pamela J. Wisniewski. 2021. Examining Collaborative Support for Privacy and Security in the Broader Context of Tech Caregiving. Proceedings of the ACM on Human-Computer Interaction 5, CSCW2: 1–23. https://doi.org/10.1145/3479540

[22] Celine Latulipe, Ronnie Dsouza, and Murray Cumbers. 2022. Unofficial Proxies: How Close Others Help Older Adults with Banking. Conference on Human Factors in Computing Systems - Proceedings. https://doi.org/10.1145/3491102.3501845

[23] Chaiwoo Lee and Joseph F. Coughlin. 2015. PERSPECTIVE: Older Adults' Adoption of Technology: An Integrated Approach to Identifying Determinants and Barriers. Journal of Product Innovation Management 32, 5: 747–759. https://doi.org/10.1111/jpim.12176

[24] Steven McElwee, George Murphy, and Paul Shelton. 2018. Influencing Outcomes and Behaviors in Simulated Phishing Exercises. Conference Proceedings - IEEE SOUTHEASTCON 2018-April. https://doi.org/10.1109/SECON.2018.8479109

[25] Tamir Mendel. 2019. Social help: developing methods to support older adults in mobile privacy and security. In Adjunct Proceedings of the 2019 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2019 ACM International Symposium on Wearable Computers, 383–387. https://doi.org/10.1145/3341162.3349311

[26] Tamir Mendel, Debin Gao, David Lo, and Eran Toch. 2021. An Exploratory Study of Social Support Systems to Help Older Adults in Managing Mobile Safety. In Proceedings of the 23rd International Conference on Mobile Human-Computer Interaction, 1–13. https://doi.org/10.1145/3447526.3472047

[27] Tamir Mendel, Roei Schuster, Eran Tromer, and Eran Toch. 2022. Toward Proactive Support for Older Adults: Predicting the Right Moment for Providing Mobile Safety Help. ACM Interact. Mob. Wearable Ubiquitous Technol 6, 1: 25. https://doi.org/doi.org/10.1145/35172491

[28] Tamir Mendel and Eran Toch. 2017. Susceptibility to social influence of privacy behaviors: Peer versus authoritative sources. In Proceedings of the ACM Conference on Computer Supported Cooperative Work, CSCW, 581–593. https://doi.org/10.1145/2998181.2998323

[29] Tamir Mendel and Eran Toch. 2019. My Mom was Getting this Popup: Understanding Motivations and Processes in Helping Older Relatives with Mobile Security and Privacy. Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies 3, 4: 1–20. https://doi.org/10.1145/3369821

[30] Tamir Mendel and Eran Toch. 2022. Meerkat: A Social Community Support Application for Older Adults. Conference on Human Factors in Computing Systems - Proceedings. https://doi.org/10.1145/3491101.3519909

[31] Savanthi Murthy, Karthik S Bhat, Sauvik Das, and Neha Kumar. 2021. Individually Vulnerable, Collectively Safe: The Security and Privacy Practices of Households with Older Adults. 5, April: 1–24. Retrieved from https://doi.org/10.1145/3449212

[32] Subigya Nepal, Weichen Wang, Vlado Vojdanovski, Jeremy F. Huckins, Alex Dasilva, Meghan Meyer, and Andrew Campbell. 2022. COVID Student Study: A Year in the Life of College Students during the COVID-19 Pandemic Through the Lens of Mobile Phone Sensing. Conference on Human Factors in Computing Systems - Proceedings. https://doi.org/10.1145/3491102.3502043

[33] Novia Nurain, Chia Fang Chung, Clara Caldeira, and Kay Connelly. 2021. Hugging with a Shower Curtain: Older Adults' Social Support Realities during the COVID-19 Pandemic. Proceedings of the ACM on Human-Computer Interaction 5, CSCW2. https://doi.org/10.1145/3479607

[34] Daniela Oliveira, Harold Rocha, Huizi Yang, Donovan Ellis, Sandeep Dommaraju, Melis Muradoglu, Devon Weir, Adam Soliman, Tian Lin, and Natalie Ebner. 2017. Dissecting spear phishing emails for older vs young adults: On the interplay of weapons of influence and life domains in predicting susceptibility to phishing. Conference on Human Factors in Computing Systems - Proceedings 2017-May: 6412–6424. https://doi.org/10.1145/3025453.3025831

[35] Kane Pepi. 2015. Text Marketing Vs. Email Marketing: Which One Packs a Bigger Punch? business2community.

[36] Erika Shehan Poole, Marshini Chetty, Tom Morgan, Rebecca E. Grinter, and W. Keith Edwards. 2009. Computer help at home: Methods and motivations for informal technical support. In Conference on Human Factors in Computing Systems - Proceedings, 739–748. https://doi.org/10.1145/1518701.1518816

[37] Elissa M Redmiles, Sean Kross, and Michelle L Mazurek. 2016. How I learned to be secure: A census-representative survey of security advice sources and behavior. In

Proceedings of the ACM Conference on Computer and Communications Security, 666–677. https://doi.org/10.1145/2976749.2978307

[38] Elissa M. Redmiles, Amelia R. Malone, and Michelle L. Mazurek. 2016. I Think They're Trying to Tell Me Something: Advice Sources and Selection for Digital Security. Proceedings - 2016 IEEE Symposium on Security and Privacy, SP 2016: 272–288. https://doi.org/10.1109/SP.2016.24

[39] Borja Sañudo, Curtis Fennell, and Antonio J. Sánchez-Oliver. 2020. Objectively-assessed physical activity, sedentary behavior, smartphone use, and sleep patterns preand during-COVID-19 quarantine in young adults from Spain. Sustainability (Switzerland) 12, 15: 1–12. https://doi.org/10.3390/SU12155890

[40] Steve Sheng, Bryant Magnien, Ponnurangam Kumaraguru, Alessandro Acquisti, Lorrie Faith Cranor, Jason Hong, and Elizabeth Nunge. 2007. Anti-Phishing Phil. 88. https://doi.org/10.1145/1280680.1280692

[41] Donghoon Shin, Subeen Park, Esther Hehsun Kim, Soomin Kim, Jinwook Seo, and Hwajung Hong. 2022. Exploring the Effects of AI-assisted Emotional Support Processes in Online Mental Health Community. Association for Computing Machinery. https://doi.org/10.1145/3491101.3519854

[42] Alison Simpson. 2022. SafeUp: How one app is helping women feel safe in London. We Are the City. Retrieved August 16, 2022 from https://wearethecity.com/safeup-how-one-app-is-helping-women-feel-safe-in-london/

[43] H. Jeff Smith, Sandra J. Milberg, and Sandra J. Burke. 1996. Information Privacy: Measuring Individuals' Concerns about Organizational Practices. MIS Quarterly 20, 2: 167. https://doi.org/10.2307/249477

[44] Katta Spiel, Oliver Haimson, and Danielle Lottridge. 2019. How to do better with gender on surveys: A guide for HCI researchers. Interactions 26, 4: 62–65. https://doi.org/10.1145/3338283

[45] Shaoxiong Sun, Amos A. Folarin, Yatharth Ranjan, Zulqarnain Rashid, Pauline Conde, Callum Stewart, Nicholas Cummins, Faith Matcham, Gloria Dalla Costa, Sara Simblett, Letizia Leocani, Femke Lamers, Per Soelberg Sørensen, Mathias Buron, Ana Zabalza, Ana Isabel Guerrero Pérez, Brenda W.J.H. Penninx, Sara Siddi, Josep Maria Haro, Inez Myin-Germeys, Aki Rintala, Til Wykes, Vaibhav A. Narayan, Giancarlo Comi, Matthew Hotopf, and Richard J.B. Dobson. 2020. Using smartphones and wearable devices to monitor behavioral changes during COVID-19. Journal of Medical Internet Research 22, 9: 1–19. https://doi.org/10.2196/19992

[46] Zhiyuan Wan, Lingfeng Bao, Debin Gao, Eran Toch, X I N Xia, Tamir Mendel, and David Lo. 2019. AppMoD: Helping Older Adults Manage Mobile Security with Online Social Help. Proc. ACM Interact. Mob. Wearable Ubiquitous Technol. 3, 4: 23. https://doi.org/https://doi.org/10.1145/3369819

[47] Yang Wang, Pedro Giovanni Leon, Kevin Scott, Xiaoxuan Chen, Alessandro Acquisti, and Lorrie Faith Cranor. 2013. Privacy nudges for social media: An exploratory facebook study. WWW 2013 Companion - Proceedings of the 22nd International Conference on World Wide Web: 763–770.

[48] Hue Watson, Eyitemi Moju-Igbene, Akanksha Kumari, and Sauvik Das. 2020. "We Hold Each Other Accountable": Unpacking How Social Groups Approach Cybersecurity and Privacy Together. In Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, 1–12. https://doi.org/10.1145/3313831.3376605

[49] Zikai Alex Wen, Zhiqiu Lin, Rowena Chen, and Erik Andersen. 2019. What.Hack: Engaging Anti-Phishing Training through a Role-playing Phishing Simulation Game. Conference on Human Factors in Computing Systems - Proceedings: 1–12. https://doi.org/10.1145/3290605.3300338

[50] Yuxi Wu, W. Keith Edwards, and Sauvik Das. 2022. SoK: Social Cybersecurity. Proceedings - IEEE Symposium on Security and Privacy 2022-May: 1863–1879. https://doi.org/10.1109/SP46214.2022.9833757

[51] 2020. Check Point Research: COVID-19 Pandemic Drives Criminal and Political Cyber-Attacks Across Networks, Cloud and Mobile in H1 2020. Check Point Software Technologies Ltd. Retrieved August 12, 2022 from https://www.checkpoint.com/press/2020/check-point-research-covid-19-pandemic-drives-criminal-and-political-cyber-attacks-across-networks-cloud-and-mobile-in-h1-2020/

A APPENDICES

A A.1 CONSENT FORM

I declare that I consent to participate at the Meerket user study, and that <name of the researcher> had explained the objectives, procedures, and risks of the study.

1. The objective of the study is to analyze the effectiveness of peer support in mobile interactions when receiving suspicious text messages.
2. The participating population are pairs that have existing social relationship, aged above 18 years, and have a smartphone that matches the configuration of our system.
3. The main personal benefit from your participation is the compensation provided at the end of the study. Receiving the full compensation will depend on executing the study procedure listed below. Apart from that, the knowledge received may be of value to humanity and hopefully the development of further privacy and security mechanisms.
4. The Study Procedure includes answering an onboarding interview, installing the Meerkat app, using the app for a week, requesting, or providing support, answering questionnaires after each support interaction, and filling in an exit interview. The participation depends on the results of the onboarding interview. All communication between the study participants regarding support interactions should be carried out in the Meerkat app.
5. The study requires installing the Meerkat app from the Google Play Store. The app will collect the following information that would be stored and used by the researchers for specific objectives that would be detailed below. The collected information includes:
    a. Phone number: the phone number will be stored to identify the user and to contact them if necessary.
    b. Screenshots: Meerkat allows users to capture screenshots of their phone. The user needs to explicitly capture, annotate, and send the screenshots to specific people. The user can also remove parts of the screenshots to hide sensitive parts.
    c. Message content: the messages sent through Meerkat will be stored.
    d. Information about using Meerkat, including times of use and log information from the app.
    e. The information from questionnaires
6. The Meerkat application will use data communication. The mobile device should be connected to either WiFi or cellular communication. Meerkat uses communicates common amounts of data, and we would like to make it clear that the research team will not pay for charges resulting from data communication.
7. You are required to use the app according to the local laws. Do not use the application while driving or in any other situations that may compromise yours, or others', safety.
8. During the use of Meerkat, you will be asked to interact with other study participants. We detail in the following guidelines the required behavior. Not following the guidelines may be a reason to terminating your participation in the study:
    a. Do not share your personal information (name, email, ID number) with other participants that you don't know already.
    b. Be respectful and kind to other participants.
    c. Do not share screenshots or information that include sensitive information or content that may make others uncomfortable.
    d. Use the app only for its intended purposes.
9. The risks and discomfort associated with participation in this study include data leakage and loss of privacy. However, the system is designed to safeguard your privacy using

state-of-the-art security and privacy enhancing technologies, including cryptographic communications and secured databases.

10. Your confidentiality will be maintained in the following manner: By participating, you understand and agree that the data and information gathered during this study may be used by <institution> and published and/or disclosed by <institution>. However, your name and other direct personal identifiers will not be mentioned in any such publication or dissemination of the research data and/or results by <institution>. However, <institution> may be required to disclose your consent form, data and other personally identifiable information as required by law, regulation, subpoena or court order.
11. Your rights: Your participation is voluntary. You are free to stop your participation at any point. Refusal to participate or withdrawal of your consent or discontinued participation in the study will not result in any penalty or loss of benefits or rights to which you might otherwise be entitled. You can contact us during or after the study, you can contact the research staff to view or to delete your data.
12. Right to Ask Questions & Contact Information: If you have any questions about this study, you should feel free to ask them. If you have questions, desire additional information, or wish to withdraw your participation please contact the Principle Investigator by email or phone.

By indicating this option, you declare that you have read and understood the above information and that you agree to participate in this research study.

B A.2 QUESTIONNAIRES

The seeker and the helper were asked to answer an initial questionnaire (onboarding):

1. What is your first name?
2. What is your last name?
3. What is your phone number?
4. What is your birth year?
5. What is your gender? Female, male, or prefer not to say
6. What is your highest academic degree?
7. Did you study a technology degree (such as computer science or engineering)
8. What is the operation that you have on your smartphone?
9. How many hours a day, on average, do you use your smartphone?
10. How well do you know the expressions related to smartphones and computers?
11. The text I sent successfully described the problem I encountered
    a. Spam
    b. Cookie
    c. Application Permissions
    d. Virus
    e. Two-step verification
    f. Remote login
    g. Setting preferences
    h. Wifi
    i. GPS
12. Below are statements about how you manage your personal information. Regarding personal information privacy, please indicate how much you agree or disagree with each statement.
13. It usually bothers me that apps ask me for personal information.
14. When apps ask me for personal information, I sometimes think twice before giving it.
15. It bothers me to give personal information to so many apps.
16. I am concerned that apps are collecting too much personal information about me.
17. Read each statement and choose the most appropriate number to the right of the statement to indicate how often you engaged in each activity (frequently Likert scale).
    a. If I discover a security problem, I keep doing what I am doing because I assume someone else will fix it.
    b. When someone sends me a link, I open it to be sure where it goes.
    c. When I browse websites, I move my mouse over links to see where they go before I click on them.
    d. I know what website I'm visiting based on its look and feel and not by looking at the URL bar.
    e. I send information to websites to ensure it is sent securely (e.g., SSL, HTTPS).
18. What is the full name of your experiment partner?
19. What is your partner's phone number?
20. What is your relationship with your experiment partner?
21. Do you live in the same house as your partner? (yes or no)
22. Installing the Meerkat app: You must install and create an account in the Meerkat application on your Android smartphone. Please approve that you install Meerkats on your Android device.

After each task, we displayed a questionnaire, one for the seeker and the other for the helper.

<source> can be either a social contact or a community member.

The seeker questionnaire after each task:

1. Would you perform what was written in the response you received from <relationship type> if the message was displayed on your device? Yes, I will do it. No, I won't do it. I don't know
2. Answer the following questions regarding the question and screenshot you sent and the last reply you received from <source>. For each statement below, choose the correct (agreement Likert scale) answer for you.
    a. The text I sent successfully described the problem I encountered
    b. The screenshot I sent helped me explain the text in a more straightforward way
    c. The text I received from <source>successfully explained the problem I encountered
    d. The drawings I received from <source> helped me to understand how to perform the task
    e. The answer I received in support from <source>helped me learn how to do the task
    f. It bothers me that <source>was exposed to sensitive information during support

g. I could handle the presented task well even without support from <source>
h. I am satisfied with the ease of the support process, from sending the questions to receiving the answer
i. I am satisfied with the duration of the support process, from sending the questions to receiving the answer
j. I am satisfied with the information I received in response as a result of sending the questions

The helper questionnaire after each task:

1. Do you think your answer will be performed on the mobile device of <source> who asked for help? Yes, I will do it. No, I won't do it. I don't know
2. Please answer the following questions regarding the question and screenshot you sent to <source>. For each statement below, choose the correct (agreement Likert scale) answer for you.
   a. The language that <source> used was clear to me that the seeker was asking for support
   b. The text written by <source> successfully described the problem he encountered
   c. The screenshot sent by <source> helped me understand the text in a more straightforward way
   d. The text I sent successfully explained the problem <source> encountered
   e. The drawings on the screenshot I sent to <source> were clear to understand how to do the task
   f. My answer allowed <source> to learn how to perform the task
   g. I was exposed to sensitive information related to <source> during support
   h. The <source> can handle a text message even without support
   i. I am satisfied with the ease of the support process, from receiving the questions to sending the answer
   j. I am satisfied with the duration of the support process, from receiving the questions to sending the answer
   k. I am satisfied with the information I provided when sending the answer

The helper exit questionnaire:

1. How often would you like to use the experiment app to help people with mobile devices? (Frequency Likert scale)
2. For each of the statements below, answer in context the questions and screenshots you received and the answers you sent to a relative or close friend. Choose the right answer for you (agreement Likert scale).
   a. I felt safe to provide support in the experiment app to a relative or close friend.
   b. I felt safe sending screenshots in the experiment app to a relative or close friend.
   c. I felt safe sending a text message in the experiment application to a relative or close friend.
   d. I taught the relative or close friend well through the experimental application.
3. For each statement below, we contextualize the questions and screenshots you received and the responses you sent to a community member. Choose the right answer for you.
   a. I felt confident in supporting the experiment app to a community member.
   b. I felt safe sending screenshots of the experiment application to a community member.
   c. I felt safe sending a text message in the experiment application to a community member.
   d. I taught the community member well through the experiment application
4. Please describe situations in which you were not available to answer questions in the application to the person seeking help.
5. Please describe the positive aspects of consistently using the app.
6. Please describe your negative aspects of the experience using the app.
7. Who do you feel you have taught among the support providers to use the experiment application? (Close connection or friend, community member, both of them, neither of them)
8. Please describe what you taught your relative or close friend through the app.
9. Please describe what you taught the community member through the app.
10. Which seekers do you prefer to support through the app for using a mobile device? (Close connection or friend, community member, both of them, neither of them)
11. Please explain your choice in the previous question regarding your preference among the applicants for support.
12. Please provide any comments about the experiment application.
13. Please provide any comments about the experiment.

The seeker exit questionnaire:

1. How often would you like to use the experiment app if you have a question about your mobile device? (Frequency Likert scale)
2. For each statement below, answer in the context of the questions and screenshots you sent and the answers you received from a close family member or friend. Choose the right answer for you.
   a. I felt safe asking a relative or close friend in the experimental application.
   b. I felt safe sending screenshots in the experimental app to a relative or close friend in the experiment app.
   c. I felt safe sending a text message in the experiment application to a relative or close friend.
   d. I learned well through the trial application from a relative or a close friend.
3. For each of the statements below, answer in context the questions and screenshots you sent and the answers you received from a community member. Choose the right answer for you.
   a. I felt safe asking the community member in the trial application
   b. I felt safe to send screenshots of the experimental application to a member of the community
   c. I felt safe to send a text message in the experiment application to a member of the community

   d. I learned well through the trial application from a friend from the community

4. Please describe situations in which you will use the application.
5. Please describe the positive aspects of consistently using the app.
6. Please describe your negative aspects of the experience using the app.
7. Who do you feel you learned from among the support providers while using the application? (Close connection or friend, community member, both of them, neither of them)
8. Please describe what you learned from your relative or a close friend through the app.
9. Please describe what you learned through the app from the community member.
10. Which helpers would you prefer to be supported through the app if you need support on your mobile device? (Close connection or friend, community member, both of them, neither of them)
11. Please explain your choice regarding your preference among the support providers in the previous question.
12. Who do you think, besides a relative, friend, and community member, can provide good support through the app?
13. Please provide any comments about the experiment application.
14. Please provide any comments about the experiment.

C A.3 PHISHING MESSAGES

We displayed ten phishing messages in randomized order:

1. The sender: City. The message: Hello, our data shows that you have a parking violation in 2nd street on April, 10th 2022 at 3:24pm. Please go to our website to obtain more information about the violation, pay your fine, or refute your ticket: www.downloadxyz.com/xyz121121
2. The sender: <Airline company name>. The message: Last opportunity! <Airline company name> is giving away two free tickets! Register today on the company website www.<airline company name>.utorrent.com/ba22212, and maybe you can win. Hurry, the raffle will take place today.
3. The sender: Maya. The message: My name is Maya. I am 62 years old. I am a learned social activist in your hometown. I arrange social activities for the elderly. I am happy to invite you to our next social meeting. To get update visit my website: www.maya.19520821898.com/agt121121. I would be happy to answer any questions.
4. The Sender: Google. The message: we recognized a new login into your account from a new device you have not logged in to before. We sent you this message to verify that it was not someone else. Login into the activity right now www.google.abc135.com/google121121.
5. The sender: Health Gov. The message: According to an epidemiological investigation, between 20:00 and 23:00, you were near a person infected by covid-19. You must fill out the form on the website of the Ministry of Health: go.gov.195abctorr.com.
6. The sender: Security. The message: According to the information we have, your mobile device is vulnerable to malicious factors. You can protect your mobile device by downloading an app at this link: http://download.torrent.com/a?i=adasde12ad.
7. The sender: Post Office. The message: Dear customer, your package number <number> is on hold due to unpaid shipping costs 27.90$. More details: http://download.torrent.com/a?i=aaade12ad.
8. The sender: Dana. The message: My name is Dana, 62. I want to keep you updated on activities, especially for you. Our site has information on shows and movies at special discounts only for seniors. To register, visit our website www.dana.19520821898.com/agt121121.
9. The sender: City. The message: Dear resident, our data indicate that you have a debt of property tax payment for February 2022. Today is the last day for the payment of the debt without arrears costs. More details can be found on the website: www.downloadxyz.com/xyz121121.
10. The sender: Google. The message: we sent you this message to verify that it was not someone else. Check out the activity right now www.google.abc135.com/google121121.