INTERVENTION EFFORTS AGAINST TECHNOLOGY ABUSE IN INTIMATE PARTNER VIOLENCE

A Thesis

Presented to the Faculty of the Graduate School

of Cornell University

in Partial Fulfillment of the Requirements for the Degree of

MSc.

by

Julia Narakornpichit

May 2020

ABSTRACT

A multi-stage study was conducted to evaluate and improve the efficacy of intervention approaches for dealing with technology-driven interpersonal attacks. Two current intervention approaches are customer support for computer security applications and notifications from mobile computer security applications. While we are specifically looking at NortonLifeLock (formerly known as Symantec)'s customer support and notification design, the improvements developed from this study can be applicable and used by other computer security companies. This work was conducted in collaboration with Yixin Zou and Allison McDonald of University of Michigan and NortonLifeLock.

CHAPTER 1

INTRODUCTION

Technology is easier to abuse now than ever through attacks such as spying and session hijacking. Tech abuse has become more common within abusive interpersonal relationships, causing physical and emotional harm to the victim. Oftentimes, the abuser has access to the victim's accounts and devices, making it easier for the abuser to exploit technology to stalk and harm the victim. In settings of intimate partner violence, technology can be misused through ownership-based access, where the abuser has access by being the owner of the device or account or through shared accounts and uses the access to digitally control access or track the victims' location, monitor their usage, among other methods. The abuser can also compromise the victim's account or device through hacking the device or forcing the victim to reveal passwords. The abuser can then install spyware on the victim's device, monitor the victim through a dual-use application that is considered to be "legitimate," track the victim, or monitor the use of the victims' accounts.

Computer security companies, such as NortonLifeLock (formerly known as Symantec), aim to help customers secure their devices, ensuring that they are free of malware and privacy threats. However, they are currently not equipped to handle such cases of security violations for vulnerable populations. NortonLifeLock currently has two intervention efforts: notifications within their mobile security app, Norton Mobile Security, and customer support, who handles cases when victims contact them about security and privacy issues that they face. Norton Mobile Security sends notifications when a user scans their device and when spyware is detected. However, if the abusers happens to see the

spyware alert, it could pose as a potential safety threat to the victim. When victims contact Norton's customer support about the security issues that they face, customer support provides technology solutions for their software. However, customer support could potentially assist victims of IPV by notifying them of potential safety issues and providing them with resources for safety planning and social work resources.

CHAPTER 2
RELATED WORK

Social workers and healthcare professionals have been providing services and support to victims of intimate partner violence and have developed many tools for abuse detection and intervention. According to a 2018 US Preventative Services Task Force study, the following tools have reasonable accuracy to detect exposure of IPV in the past-year in adult women: Humiliation, Afraid, Rape, Kick (HARK), Hurt/Insult/Threaten/Scream (HITS), Extended Hurt/Insult/Threaten/Scream (E-HITS),Partner Violence Screen (PVS), and Woman Abuse Screening Tool (WAST). These tools primarily focus on whether or not a potential victim has experienced physical violence or emotional victimization. The United States Department of Health Human Service's Office on Women's Health provided the following checklist for potential victims of intimate partner violence to determine if they have been experiencing abuse.

- You may be experiencing domestic violence if your partner:
- Controls what you're doing
- Checks your phone, email, or social networks without your permission
- Forces you to have sex when you don't want to

- Controls your birth control or insists that you get pregnant
- Decides what you wear or eat or how you spend money
- Prevents or discourages you from going to work or school or seeing your family or friends
- Humiliates you on purpose in front of others
- Unfairly accuses you of being unfaithful
- Destroys your things
- Threatens to hurt you, your children, other loved ones, or your pets
- Hurts you physically (e.g., hitting, beating, punching, pushing, kicking), including with a weapon
- Blames you for his or her violent outbursts
- Threatens to hurt herself or himself because of being upset with you
- Threatens to report you to the authorities for imagined crimes
- Says things like, "If I can't have you, then no one can"

Many national and local hotlines and organizations exist for supporting victims of intimate partner violence, such as Rape, Abuse Incest National Network (RAINN), the National Domestic Violence Hotline, and Safe Horizon. Similar to customer support lines, these organizations take calls from victims of abuse asking for help and provide interventions. After a victim of IPV is identified by the hotline, the victim is connected with a local sexual assault service provider that can assist with things such as counseling, medical attention, legal advocacy, education, and shelters.

In addition, healthcare professionals are provided with tools to handle victims of domestic violence. Stanford Medical provides checklists for tips on how

to ask potential victims written questions, as well as oral questions. They provide questions that allow healthcare professionals to screen for IPV directly (ie, "Are you afraid of your partner? Do you feel you are in danger?") and indirectly (ie, How are things going at home?) and ways to frame questions (ie, "From past experience with other patients, I'm concerned that some of your medical problems may be the result of someone hurting you. Is that happening?"). The guide highlights being non-judgemental and supportive in responses, and provides suggestions for how to respond (ie, "It's not your fault." "I'm very glad you told me. I care. I'm concerned about the health and safety of you and your children.") and how not to respond (""If it were me, I wouldn't put up with this."). These existing methods can be incorporated into how technology security companies interact with victims of intimate partner violence.

CHAPTER 3
METHOD

A study was conducted to understand how technology security companies should provide safer user experiences for people experiencing intimate partner violence. We focused on the two existing interventions, customer support and privacy risk notifications within security applications. We wanted to understand how customer support can better handle cases with victims of intimate partner violence and how notifications within mobile security applications can be designed in a way that would not endanger the victim. In order to do so, focus groups were held with professionals who work with victims of intimate partner violence. The focus groups were asked questions about practices customer support should employ to support victims of IPV and how the current design of notifications can be improved.

3.1 Mobile Security Application Review

In order to understand the design of mobile security applications, in addition to Norton Mobile Security, two other popular mobile security applications were reviewed: Avast Mobile Security and Kaspersky Internet Security. We looked at multiple security applications to elucidate design principles for security applications and their notifications. We aimed to understand if the applications were similarly flawed, as well as the good and bad aspects of the design of each application.

First, an informal review of the three applications were conducted to familiarize ourselves with the security applications and to catch glaring issues with applications. A corpus of spyware applications were downloaded to a Samsung Galaxy Android device to trigger the security applications. Each app was prompted to scan the device, and the screens related to the scan, such as the screen showing the scan in progress and the screens with the results, as well as the notifications were reviewed. Other aspects of the user interface including the help section were reviewed as well. These functions were selected to be reviewed as they pertained to the detection of spyware on the device, thus, relevant to the study.

Next, we conducted an heuristic evaluation of existing mobile security applications Kaspersky Internet Security, Norton Mobile Security, and Avast Mobile Security using Jacob Nielsen's 10 Usability Heuristics for User Interface Design. We attempted to find another set of heuristics that focused on the design challenges faced by security applications, but were unsuccessful. We ranked each heuristic for each app on a scale from 1 to 3, where 1 is a negative score, 2 is a

neutral score, and 3 is a positive score. The heuristic evaluation was conducted to identify existing problems with the applications and to prioritize what should be asked about in the focus group.

3.2 Focus Groups

The user at the focus of the study are victims of intimate partner violence. However, they are considered to be a vulnerable population and may not provide enough or accurate data. Such victims may withhold information because they do not feel safe or are in denial. In addition, studying this user may put them in danger. Instead of recruiting the users for the study, professionals and advocates for victims of intimate partner violence and domestic violence were studied. Focus groups consisting of two to three professionals and advocates were held with professionals from New York City based organizations, Sanctuary for Families and Mayor's Office to End Domestic and Gender-Based Violence. The discussions with the focus groups lasted an hour long and followed the protocol that we developed, which included a brief overview about the study for context, a discussion around the three customer support scenarios, and a discussion around the design of mobile anti-virus applications. The participants were given a form for providing demographic information, which included their gender, age range, and profession. Notes and an audio recording were taken during the duration of the focus group.

3.2.1 Protocol for IPV Expert Focus Groups

The protocol consisted of three parts: an introduction, a discussion surrounding three scenarios from NortonLifeLock customer support, and a discussion around the design of mobile anti-virus applications, with a focus on the notifications. (The full protocol can be viewed in Appendix A.) The introduction provided the professionals with background on the study and NortonLifeLock and included warm-up questions for us to establish rapport with the professionals. These questions were introductions about the backgrounds of the professionals and their experiences with clients experiencing intimate partner violence. Following the introductions, the professionals were presented with a three example transcripts between a customer and a customer support agent. These transcripts are transcripts of real conversations between customers and agents of NortonLifeLock that have been shortened and scrubbed of identifying information. In all three scenarios (Appendix A), the customer is in an unsafe situation with a partner that involves predatory usage of technology, such as hacking or spying. The professionals are then prompted with questions about advice that they recommend to be given to the customer given the scenario, advice given to customer support on how to handle the given scenarios, and general advice to customer support. Questions that provoked further discussion about situations that could complicate the advice or scenario were asked as well. These questions considered what the customer support representative should do if the attacker is recording or listening to the support chat, if the customer/victim is not alone when the call takes place, and if the attacker is impersonating the victim to gain access to the victim's account.

Lastly, the professionals are presented with a sheet with screenshots of no-

tifications from Kaspersky Internet Security, Avast Mobile Security, and Norton Mobile Security, alerting the user of malware being detected on their device, and screenshots of the user interface of the applications. They are asked to review and provide feedback for the screenshots, as well as advice they would give victims when they are alerted. In addition, they are asked to consider what can be done so the notifications do not put victims in additional danger if the abuser sees the notification.

CHAPTER 4

RESULTS

4.1 Heuristic Analysis of Mobile Security Applications

We conducted heuristic analyses of the three mobile security apps.

4.1.1 Avast

Avast did well on the visibility of the system status, as the scan shows the number of threats found so far and the percentage of completeness. Avast received a negative ranking for ”match between system and the real world,” since it was unclear what was a threat and what was a risk. Avast received a positive score on user control and freedom, since the user can ignore things that the app detects as malware and go back to find previously ignored malware. Avast received a neutral score for consistency and standards, aesthetic and minimalist design, flexibility and efficiency of use, help users recognize and recover from errors, help and documentation, and recognition rather than recall. It was

clear how to scan the app, but it was hard to differentiate the ”file scanner” and ”scan” features. It was also unclear what ”resolve” means in the malware interface. However, when the user clicked on ”resolve,” it asked the user to uninstall the app.

4.1.2 Kaspersky

Kaspersky received a positive score for ”Visibility of system status,” since the status bar made it clear that the scan was happening. However, it received a negative score for match between system and the real world, since it did not provide a clear explanation for why an app is considered a risk. The notifications also showed no difference in descriptions between a ”Threat detected!” alert and a ”Privacy alert!” The description of what apps were detected were often incomprehensible. The app received a negative score for ”User control and freedom” because it forces the user to delete or skip threats that are detected as they are detected, and pauses the scan until they are handled. In addition, there is no way to view the alerts that are skipped. It received neutral scores for consistency and standards, error prevention, and flexibility and efficiency of use. It also received a negative score for recognition rather than recall because the app provides a summary of the scan once it is finished, but no list or details are provided on the threats that were detected and the apps that were skipped. The user has to re-scan to find the information again. In addition, the user is unable to see what apps were quarantined. It is also unclear what that means.

4.1.3 Norton

Norton received a neutral score for visibility of system status. The app showed the progress of the scan, when the system is scanned. However, when the scan is completed, it disappears and doesn't notify the user of its completion. It received a negative score for "match between system and the real world." It was unclear what was considered anti-malware, what was considered a privacy risk, and what was considered "anti-theft." In addition, it also received a negative score for user control and freedom because a "malware found" notification remains in the lock screen until all malware is resolved. In addition, there is no option to ignore malware or report as false positive. The user can only delete malware. The app received a positive score for error prevention, as the user needs to confirm twice before uninstalling an app. It received neutral scores for recognition rather than recall, flexibility and efficiency of use, and help and documentation.

4.2 Focus Groups with Intimate Partner Violence Professionals

So far, two focus groups have been conducted with professionals at the Sanctuary for Families and Mayor's Office to End Domestic and Gender-Based Violence. Both focus groups had a lot of feedback to provide about the customer support scenarios and the notifications. Many questions were answered by the professionals before they were asked, which caused asking all the questions in the protocol to be unnecessary.

4.2.1 Customer Support

From the two focus groups conducted so far, both set of professionals felt that the customer support representatives handled the cases poorly. Both groups noted that the customer service representative should not promise to resolve the issue, as they did in Scenario A. They believed that customer service representatives should undergo empathy training to learn how to respond to cases that involve abuse and trauma in an empathetic manner. They suggested having a list of key words or red flags that could indicate that the customer is a part of a vulnerable population or potentially a victim of intimate partner violence. Both groups suggested transferring cases that mentioned abuse or contained the keywords or red flags directly to hotlines for domestic violence after the representative has helped the customer with their tech problem. They also mentioned providing the customer with resources for help, and acknowledged that there is a chance that the customer might drop off the line before they are transferred or may not want the resources provided.

In addition, both groups noted that there should be a group of professionals within the customer support team that are ideally trained in social work to handle cases involving abuse and intimate partner violence. Any cases with certain keywords or red flags would be transferred to this group of professionals, who would handle the case.

4.2.2 Notifications

Both groups agreed that designing notifications that were safe for victims of IPV and did not alert the abuser was a challenging problem. They were unable to of-

fer many solutions. Almost immediately, both groups noted that the language of the notifications would be triggering to victims, as they involved alarming language such as ”Warning! Issues detected.” This language may cause victims to panic and feel unsafe. Both groups mentioned the need for plain language that was easy for the user to understand and clear. For example, one notification (see Figure 1) included ”unusual app behaviors” and ”phone monitoring,” which was unclear. However, both groups liked the in-app notification provided by Kaspersky (see Figure 2), which contained clear and informative language. One group suggested including a ”safe notifications” setting that would mask the notifications. For example, instead of showing a malware scan notification, the victim would receive notifications about a weather application. The victim would be aware that the notification was from the mobile security application, however, the attacker would not. They also suggested sending notifications about malware via email or text, instead of as a notification. Another group suggested not having notifications at all, requiring the user to check the application for alerts.

CHAPTER 5
DISCUSSION

5.1 Customer Support

The focus groups suggested that the customer support representatives should be given empathy. The methods provided by Stanford Medical in their lists of how to ask questions and respond to victims of intimate partner violence, which were created for medical professionals, could be helpful and serve as guidelines

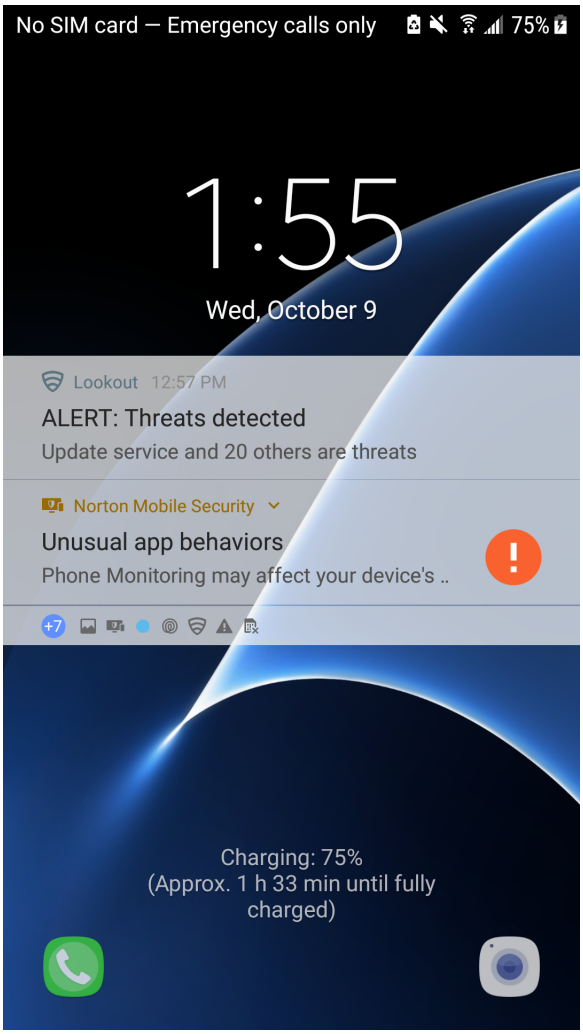

Figure 4.1: Norton Lock Screen Notification

for customer service representatives when they speak to potential victims of IPV. While the IPV screening tools detailed in the Related Work section may not be appropriate for the customer service representatives to use during their chats, customer service representatives can look for key words, as the focus group mentioned, and those key words can include similar flags as those in the IPV screening tools. In addition, the red flags for Domestic Violence provided by New York State's Office of Addiction Services and Supports, could be helpful for customer service to detect customers that are IPV victims. For example, red

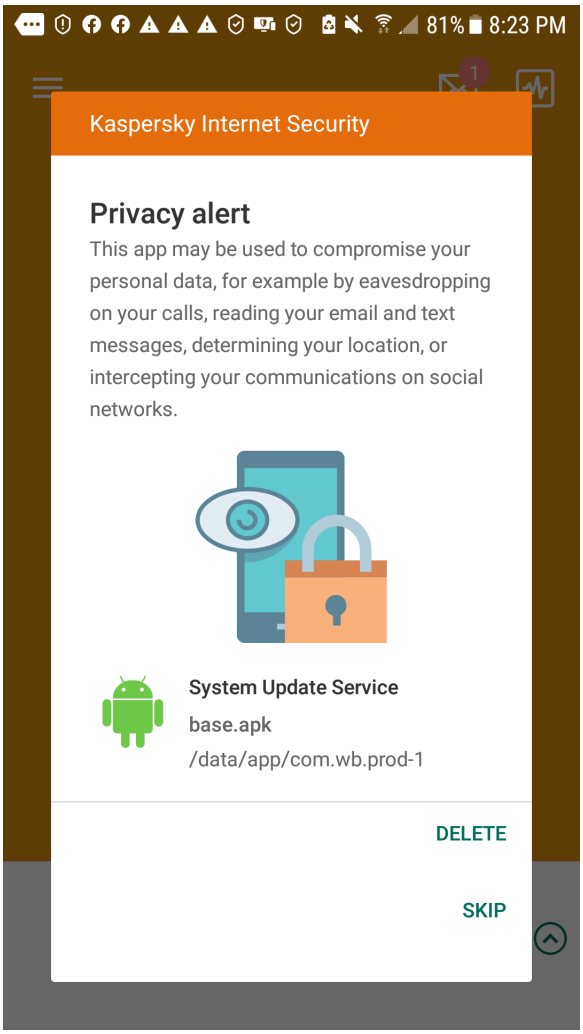

Figure 4.2: Kaspersky In-App Notification

flags on the list include confusion, fear, and self-blame and suicidal thoughts.

5.2 Notifications

From the heuristic evaluation, common issues that were found among all platforms included use of jargon and confusing language, lack of features to support efficiency of use, inability to undo actions, such as accidental removals of apps,

and clear explanations for why certain apps were flagged. The focus groups agreed with our assessment that confusing language and jargon used was an issue with the mobile security applications. The language used within the mobile security apps must be changed not only to be less alarming, per the IPV professionals' recommendation, but also to have clear and informative language that is easy to understand. The apps also need to be easier to navigate. For example, Kaspersky and Norton should provide a detailed log of the scans after it is completed. Also, Kaspersky should not stop the scan when one item is detected, waiting for it to be resolved before continuing.

From our analysis, we noticed that there are many general usability problems with these apps. For example, the language can be too technical or unclear and it is often unclear what risks a detected app poses. While this can lead to frustration and confusion in the general user, it can cause panic or fear within a victim of IPV who believes they are being tracked by their partner.

5.3 Limitations

The mobile security application portion of the study was conducted only on Android devices. We have not studied how the notifications and user interface and experience differ on the iOS devices. Thus, it is unclear if the results from the heuristic analysis of the three mobile applications applies to the corresponding iOS applications. The results of the security application portion and corresponding advice from the IPV professionals also may not apply to desktop security applications, due to the design of such applications and the nature in which laptops and desktop computers are used. The findings from the heuristic

analysis of the mobile security applications is also limited to the three applications mentioned: Norton Mobile Security, Avast Mobile Security, and Kaspersky Internet Security.

In addition, this work is ongoing. Data from professionals are still being collected. Not enough data has been collected for conclusive results or for a recommendation to be developed for security companies.

5.4 Future work

This work is ongoing. Within the upcoming months, more in-person focus groups with IPV professionals from New York City based organizations, such as Safe Horizon, will be conducted to gather more insights on methods for customer service teams at computer security teams to adopt, as well as suggestions on how to improve notification design for victims of IPV. The qualitative data from these sessions will be compiled, coded, and analyzed. The data from the analysis will be used to develop a plan for customer service for computer security companies to become better equipped to handle cases from victims of intimate partner violence and a design strategy for notifications of anti-virus and mobile security apps (i.e., Norton Mobile Security, Avast Mobile Security, and Kaspersky Internet Security) with IPV victims in mind. We plan to propose the plan and design strategy to NortonLifeLock for their customer service team and anti-virus applications to adopt. Our work will be compiled in a paper and submitted to the ACM Conference on Computer-Supported Cooperative Work and Social Computing in 2020.

CHAPTER 6

CONCLUSION

With more technologies available for cyberstalking, it is important for cybersecurity companies, like NortonLifeLock, to protect populations that are vulnerable to such technology abuse, like victims of intimate partner violence. We conducted a study to understand how technology security companies improve two intervention methods: customer support and mobile security application notifications. First, we conducted reviews and heuristic analyses of three mobile security applications: Norton Mobile Security, Avast Mobile Security, and Kaspersky Internet Security. We discovered many usability issues, including use of jargon and confusing language, little support of re-dos when the user accidentally resolves an issue, and lack of features to support efficiency of use. We developed a protocol for focus groups with professionals working with intimate partner violence victims to understand how to improve the customer support experience and design of notifications for victims of IPV. This protocol was used with in two focus groups. The focus groups noted that customer support teams should be given empathy training and have a set of key words that would flag certain customers as potential victims of intimate partner violence. Those potential victims should be provided resources. In addition, the language used within the notifications of mobile security apps should not include jargon, be clear, and not alarmist. More focus groups will be conducted in the future. The data from these focus groups will be used to develop a plan for technology security companies to use for their customer support teams and a design strategy for the notifications of their mobile security applications

BIBLIOGRAPHY

APPENDIX A

NOTIFICATION SHEET FOR FOCUS GROUP PROTOCOL

APPENDIX B

FOCUS GROUP PROTOCOL

Part 1: Introduction and warm-up (10 minutes)

Thank you all for taking the time to talk to us. We're researchers from Cornell Tech, the University of Michigan, and NortonLifeLock (formerly known as Symantec Corporation). NortonLifeLock provides cybersecurity software and services like Norton Antivirus and Norton Mobile Security.

NortonLifeLock offers customer support hotlines and online chats to help their customers deal with tech-related issues. There are instances in which the caller appears to be in a dangerous situation, such as stalking and domestic violence. NortonLifeLock wants to better assist these callers and understand the appropriate scope for their customer support team in doing so.

Today's meeting will be primarily discussion-based with a few activities. There are no right or wrong answers to any of our questions. We're simply interested in your opinions based on your own experiences or perspectives. You can choose not to comment if you don't want to, and you can quit the session at any point.

We would also like to get your consent to audio record the workshop session as a backup of our notes. These will be transcribed, all identifying information

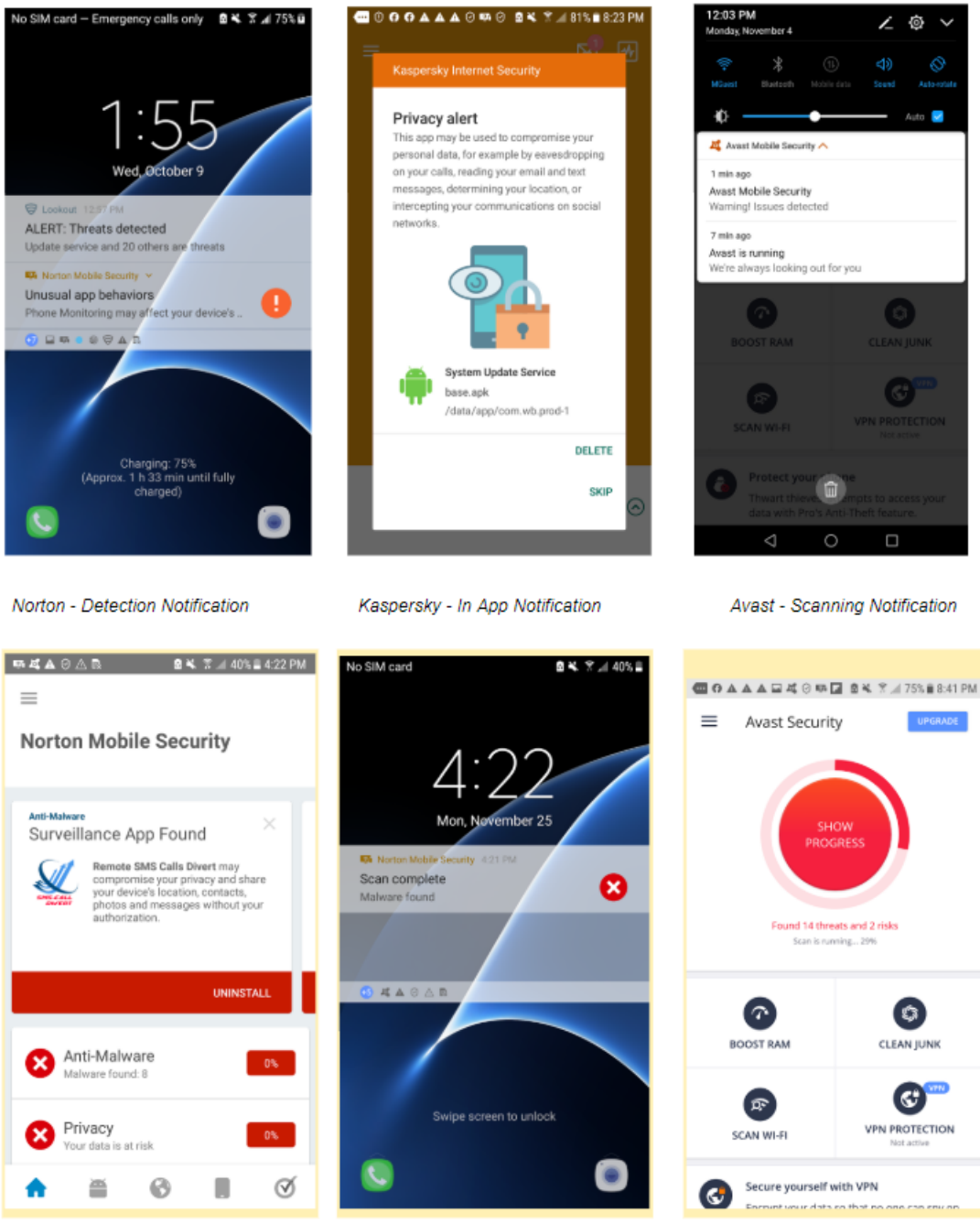

Figure A.1: Notification Sheet

will be removed, and we will destroy the original recordings once the transcription is done. Are you ok with us recording the meeting? Do you have any other questions before we get started?

[Opening questions to establish rapport, get participants talking]

- Let's go around the room with brief introductions - say your name, job title, and how many years you have been doing this job.
- Do you work directly with clients who have experienced IPV? (Have you ever worked directly with clients?)
- Have you encountered clients who have experienced tech-related abuse? Can you give an example?

Part 2: Customer Support Scenarios (10 minutes each)

Now we'd like to present a few example customer support transcripts and get your expert opinions on these interactions. These transcripts are based on real chats, but have been shortened and identifying information removed. We'll let you read each scenario and ask a few follow-up questions.

Scenario A:

Customer: My ex-husband hacked my phone. He keeps getting my account passwords. I have changed phones so many times and got a restraining order on him, but he still managed to do this. Help me please.

Support: Thank you for contacting us. I'm happy to help resolve the issue. I

would recommend installing Norton Antivirus, which should prevent malware from being installed if you get a new phone.

Customer: I have already spent a lot of money trying to fix this problem and talked to my phone provider. No one has been able to fix it. I can't spend more time and effort on this. Please help, this problem has almost driven me to commit suicide.

Support: Please do not worry about these devices if you have Norton installed. We will do everything we can to help you further.

Scenario B:

Customer: My husband is violent and keeps hacking my email and watching everything I do online. Could you help me get him off my network?

Support: I'm sorry to hear what you are going through. How do you think he is watching your activity?

Customer: He doesn't live with me anymore, but he broke into my apartment last month and I think he hacked my router. I am afraid he can see everything I am doing.

Scenario C:

Customer: My ex used to share my computer and installed some programs, but I think she installed spyware. I think she is remotely accessing my computer. Can you help?

Support: Thank you for contacting Norton, I will be happy to assist you. Let's set up a remote connection so I can scan your device for malware. Please visit this link

Customer: I can't open it. My computer just restarted. I think she is monitoring this chat and trying to stop me from getting help.

Per-Scenario Discussion

Advocate advice to this customer

Ignoring the technical aspect of this problem for a moment, imagine someone were to come to you with this problem...

- Are these problems similar to or different from the cases you normally receive at your organization? In what ways?
- What advice would you give this customer based on the available information?

Advocate advice to customer support for this customer

Now let's think about this customer's interaction with customer support...

- In your opinion, what could the customer support rep offer this customer beyond assistance with Norton products?
- Are there additional questions that customer support should be asking?
- Are there resources customer support could have shared?

If not mentioned In your opinion, should customer support point the caller to other organizations, such as family shelters or the police? Why or why not?

IF YES How should it be done?

- In your opinion, should customer support provide specific advice about safety planning? Why or why not? How might it be done?

Factors that might complicate advice

Let's discuss a few factors that make the situation trickier. For each case, should the support rep react differently in your opinion, why or why not?

- What if the support agent thinks attacker is recording or listening to the support chat?
- What if the person is not alone when the call takes place?
- What if the attacker could be the person calling to gain more access to a victim's account?

Part 3: General Advice (15 minute)

Now that we've looked at some examples of the problems that customer support gets, let's think about the broader role that customer support can play in providing support to victims of abuse.

- Under what circumstances, if any, do you think that customer support's duty to help extends beyond addressing product-specific issues identified by the customer?
- In your opinion, should customer support try to identify situations in which the caller may need additional safety planning advice (e.g., contact police, DV shelter, or other resources)? Why or why not?

IF YES What can customer support do to quickly identify such situations? For example, asking questions that you would normally ask in your role? Examples: "Have you contacted the police?", "Are you safe right now?", "Have you contacted a domestic violence hotline or shelter?"

- Should customer support watch out for cues that indicate further questions would be unsafe (e.g., the conversation might be monitored)? Why or why not?

IF YES What are examples of such cues?

- How should customer support respond if a customer reveals personal, sensitive information about an assault or about suicide?
- What training or education do you think the support rep could have to help them avoid adverse outcomes?

Probes About respectful language? About IPV and risks related to leaving an abuser? About resources to share with potential victims?

- Do you have any final thoughts about the role you think customer support should play in holistic safety planning?

Part 4: Norton Notifications (5 minutes)

This section intends to stay on a high level. We should try our best to encourage IPV experts to focus on their expertise areas (e.g., safety planning) rather than design-related issues.

For the last few minutes, we wanted to discuss a recent initiative by NortonLifeLock. Since July 2019, Norton Mobile Security has started detecting and sending in-app notifications to customers about apps on their phones that allow another individual to track them or spy on them, such as by monitoring their location, text messages, calls, or by remotely enable the camera or microphone. The ideal case for this feature is that the surveilled individual will receive this notification, realize they are being monitored, understand the nature of the monitoring, and take additional safety procedures as needed (e.g., by contacting customer support, a domestic violence hotline, or other support system). However, this is an ongoing effort, and we would like to know how to make sure this mechanism is safe for customers in these complex situations.

- What should companies consider in designing and delivering such notifications?
- What are the unique needs of IPV victims that might be different from the general users?
- What things can be done to ensure the notification is safe and does not put the victim in additional danger?
- For instance, how can we account for potential safety concerns if an abuser were to see the notification?