Navigating Traumatic Stress Reactions During Computer Security Interventions

Lana Ramjit, *Cornell Tech;* Natalie Dolci, *UW-Safe Campus;* Francesca Rossi, *Thriving Through;* Ryan Garcia, *UW-Safe Campus;* Thomas Ristenpart, *Cornell Tech;* Dana Cuomo, *Lafayette College*

https://www.usenix.org/conference/usenixsecurity24/presentation/ramjit

This paper is included in the Proceedings of the 33rd USENIX Security Symposium.

August 14–16, 2024 • Philadelphia, PA, USA

978-1-939133-44-1

Navigating Traumatic Stress Reactions During Computer Security Interventions

Lana Ramjit
Cornell Tech

Natalie Dolci
UW - Safe Campus

Francesca Rossi
Thriving Through

Ryan Garcia
UW - Safe Campus

Thomas Ristenpart
Cornell Tech

Dana Cuomo
Lafayette College

Abstract

At-risk populations need direct support from computer security and privacy consultants, what we refer to as a security intervention. However, at-risk populations often face security threats while experiencing traumatic events and ensuing traumatic stress reactions. While existing security interventions follow broad principles for trauma-informed care, no prior work has studied the domain-specific effects of trauma on intervention efficacy, nor how to improve the ability of tech abuse specialists to navigate them.

We perform a multi-part study into traumatic stress in the context of digital security interventions. We first interview technology consultants from three computer security clinics that help intimate partner violence survivors with technology abuse. We identify four challenges reported by consultants emanating out of traumatic stress, some of which appear to be unique to the digital security context. To better understand these challenges, we analyze transcripts of sessions at one of the clinics, extracting five patterns of how stress reactions affect consultations. We use our findings to develop new recommended best practices, including a new intervention protocol design to help guide security interventions.

1 Introduction

A growing body of research has highlighted the computer security and privacy needs of at-risk populations who face either increased likelihood of technology abuse or outsized harms should abuse occur [50]. Examples include survivors of intimate-partner violence (IPV) [15, 30, 48, 49], the LGBTQ+ community [29], the elderly [37], refugees [44], and human trafficking victims [11]. Each of these populations navigate unique security and privacy threats, and may disproportionately benefit from personalized expert guidance from e.g. company customer service [42, 53], technology abuse clinics [15, 30, 48], or NGOs [44]. Throughout this paper, we refer to such tailored guidance as *security interventions*, in which an expert *consultant* provides support to a *client*.

At-risk populations often seek security interventions while coping with traumatic events, such as abuse or political violence. Trauma can cause stress reactions that may have profound impact, such as fatigue, anxiety, or even hallucinations [25]. Thus, experts in security and privacy for at-risk users suggest that accessible and effective security interventions be *trauma-informed* [4, 5]. As in other service provision contexts, like trauma-informed lawyering [31] or investigation [8], this requires a domain-specific understanding of how traumatic stress affects services.

Yet, no prior work has investigated how traumatic stress impacts computer security interventions. Charting this gap is critical. Failing to account for distinct patterns of traumatic stress within security interventions risks not just inefficient service, but potential harm to client well-being. For example, a well-meaning and compassionate technology consultant might unwittingly encourage conversation that triggers anxiety attacks—or even inadvertently validate stress-induced hallucinations of technology abuse.

In this paper, we examine how traumatic stress impacts computer security interventions. We do so through a two-part study centered on three technology abuse clinics for IPV survivors. At these clinics, designed with the best trauma-informed practices available at the time, consultants work with IPV survivors experiencing technology abuse, such as account compromise by an abusive partner, potential spyware, and harassment on social media [15, 30].

The first study consisted of semi-structured interviews with 11 technology consultants across the three technology abuse clinics. Interviews sought to understand the traumatic stress reactions that manifest during client sessions, the challenges those responses present, and consultants' preparedness to navigate those challenges. The second study was conducted in collaboration with subject matter experts in mental health (hereafter, SMEs) and included qualitative analysis of 18 transcripts from sessions conducted at a technology abuse clinic. Analysis focused on patterns of traumatic stress reactions that presented during client-consultant interactions, with the SMEs providing clinically-informed explanations for these patterns. Drawing on the findings from both studies and the clinical expertise of the SMEs, we introduce six *care practices* for consultants to use during sessions and design a security intervention protocol that refines the Havron et al. [30] understand-investigate-advise protocol to concretize how these care practices can be deployed.

In doing so, we offer the following contributions:

- a cross-site examination of how technologists currently experience and respond to traumatic stress reactions,
- a model, based on primary sources, of how traumatic stress manifests during delivery of security interventions,
- a set of guidelines for trauma-informed care uniquely tailored to computer security clinics serving IPV survivors,
- and a suggested revision to existing intervention protocol, that better operationalizes trauma-informed care.

Our findings are already being incorporated into new training materials and new organizational practices at one of the three clinics. These will be disseminated to other clinics, helping improve intervention delivery.

More broadly, our findings suggest that security intervention delivery benefits from a bespoke understanding of traumatic stress reactions. Future work could explore the generalizability of our results in additional contexts including other at-risk populations or intervention sites (e.g., computer security customer support systems). Our methodological approach should be useful to guide such future work.

2 Related Work

Technology abuse in IPV. Intimate partner violence (IPV) is a widespread social ill affecting one out of three women and one out of six men at some point in their lives [46]. While perhaps most often associated with physical, sexual, or emotional violence, the majority [39] of IPV situations include some form of technology abuse: the abuser uses technology as a means to harass, surveil, control, or otherwise harm their target. While scholars refer to this phenomenon using a variety of names, in this paper we use tech(nology) abuse. [14, 36].

A now large body of literature has documented the wide range of ways in IPV abusers weaponize technology, via reports from survivors or professionals working with them [18, 27, 28, 35], as well as from online forums where abusers discuss abuse tactics [3, 47]. Examples include installing spyware onto a partner's device, using Bluetooth or GPS tracking devices, compromising email accounts, harassment via social media or text messaging, and distributing non-consensual intimate imagery (NCII). Not only is tech abuse complex aggregated across survivor experiences, but one individual may suffer from multiple forms of tech abuse [27]. At the same time, as Chen et al. [12] explore, technology abuse may be a source of trauma or re-traumatization, and traumatic stress reactions may impact peoples' technology experience.

Traditional computer security approaches, such as usability audits of account security interfaces or "smart labels" warning consumers of privacy issues for household devices, can help mitigate tech abuse [16, 20]. However, navigating the technical and emotional complexity of tech abuse remains non-trivial, and researchers and practitioners have therefore argued that we must complement those approaches with direct, personalized support for survivors experiencing technology abuse [14, 26, 30].

Human-based security interventions. Digital security mechanisms and policies are frequently complemented with what we will refer to as human-based interventions for targets of digital attacks. Here, we discuss examples of such human-based interventions, focusing on interventions provided to individuals, rather than interventions directed at organizations such as companies or non-profits.

For our purposes, a security intervention arises when a (potential) target of a digital attack enlists the assistance of a trained professional, who has both the technical expertise and access to tools that may help the victim discover and remediate the attack. Examples that can fall into this class include customer support for a product, consumer help desks like Apple's Genius bar, consumer IT tech support companies offering security services, and private forensics services.

A small amount of academic work has started investigating these kinds of commercial interventions. Sharif et al. [42] studied the types of security issues reported by individuals to a security company's customer service system, and how well those aligned with expert's perspectives on security. The study used customer service logs from NortonLifelock, a large consumer antivirus and fraud protection company. Roundy et al. [53] used the same dataset to investigate how IPV presents to customer service agents, and used semi-structured interviews to gather suggestions from IPV survivor support professionals about how to improve customer service delivery.

This paper focuses on technology abuse clinics, a newer form of security intervention that is qualitatively different from the commercial interventions described above. These clinics aim to assist specific at-risk populations with addressing technology-enabled abuse, using volunteers trained in both population-specific issues and as well as computer security best practices. The approach also goes by the moniker clinical computer security (c.f., [30]). The most mature examples of such clinics have arisen in the context of IPV [15, 30]. These clinics emanated out of academic environments, with initial evaluation of their success primarily via qualitative methods [26] and surveys [15].

Subsequently, a line of work has investigated clinic service delivery. Tseng et al. [48] analyzed a COVID19-inspired rapid shift of a clinic to operate remotely, highlighting among other findings the emotional and time management burdens, as well as the difficulty of conclusively determining explanations of client experiences, particularly as those challenges intersect with remote service delivery. Tseng et al. [49] later explored how to adopt a feminist ethic of care to enable better customizing interventions to individual IPV survivors. Their work highlights the challenges around establishing service scope boundaries, the difficulty of finding service endpoints, and the difficulty of navigating client hypervigilance in light of the typical inability to find conclusive "ground truth" that explain tech abuse experiences. Some of our findings reinforce those in [48, 49], as we will discuss in later sections. Finally, Slupska and Strohmayer [45] interview tech-abuse advocates, highlighting in particular the importance of networks of other practitioners that advocates can employ to help support survivors with specific issues.

Prior work has therefore acknowledged the complex emotional landscape of interventions, the possibility of some traumatic stress reactions, and the need to be trauma-informed. But prior work has not studied the role of traumatic stress reactions in computer security interventions.

3 Trauma and Intervention Design

In this section, we provide background on trauma and traumatic stress reactions, with a specific focus on how direct service providers incorporate trauma-informed care into their practices. We also include a composite vignette illustrating how traumatic stress reactions typically manifest in computer security clinics, then conclude by detailing how these implications influenced our study design.

Trauma and trauma-informed care. According to the United States' Substance Abuse and Mental Health Administration (SAMHSA), trauma "results from an event, series of events, or set of circumstances experienced by an individual as physically or emotionally harmful or life threatening and that has lasting adverse effects on the individual's functioning and mental, physical, social, or spiritual well-being" [25].

Exposure to IPV is associated with an increased likelihood of long-term traumatic stress reactions, with rates of post-traumatic stress disorder (PTSD) among IPV survivors estimated at 2-3 times that of the general population [17]. Even when exposure to trauma does not result in long-term effects, trauma can cause short-term *stress reactions* [25]. Some non-comprehensive examples include physical (e.g., extreme fatigue, hyper-arousal), emotional (anxiety, grief, shame, hopelessness), behavioral (avoidance of triggering situations), and cognitive (hyper-vigilance to threats, flashbacks).

Mental health clinicians have robust evidence-based approaches for supporting people experiencing stress reactions [43, 51]. This includes a range of treatments provided by licensed psychiatrists, psychologists, and social workers [21]. Yet, people experiencing traumatic stress regularly seek support from direct service providers outside of the mental health community. Mental health clinicians have played a key role in advancing trauma-informed practices for direct service providers — who are not mental health clinicians — to use in supporting people experiencing traumatic stress reactions, including survivors of IPV. This includes trauma-informed interviewing practices for law enforcement [8], trauma-informed legal advocacy in family law settings [1], and trauma-informed patient care in medical settings [40].

Regardless of the setting, a central principle guides trauma-informed IPV care: all elements of service delivery should be shaped by an understanding of how abuse impacts the lives of clients [19]. While specific approaches may vary, empathy and validation are central to the provision of trauma-informed care [33], both of which help to convey to an individual that they are heard and believed, that their emotions are rational, and that they are not being judged. Empathy and validation are also important tools for developing rapport and trust with individuals experiencing stress reactions, a crucial element for providing effective direct service support.

IPV security clinics were consciously designed to incorporate trauma-informed care practices into their service models. The technologists (referred to as consultants) receive specialized trauma-informed care training before beginning direct service work with survivors (referred to as clients) [13, 15]. These practices are further embedded within the structure of clinic sessions, beginning with the understand-investigate-advise framework developed by Havron et al. [30]. This protocol provides guidance to consultants when working with clients, suggesting that consultants "*understand* the client's technology issues, *investigate* their devices and accounts, and *advise* the client on next steps" [30]. While the entirety of the protocol is client-centered and trauma-informed, the 'understand' phase of the protocol in particular emphasizes active listening, a practice of attuning to the speaker's emotional and explicit delivery, and verbally reflecting that back to the speaker in order to both empathize with and validate the client's experiences and chief concerns.

Technology abuse clinics and stress reactions. To concretize the subtleties of navigating stress reactions when working with clients, we include below a composite example that is reflective of the authors' experiences working with hundreds of survivors of tech abuse at computer security clinics. This composite focuses on challenges associated with traumatic stress reactions that commonly emerge in a clinic session.

A client Casey is referred to a technology abuse clinic by their social worker: Casey mentioned being afraid to use their email for fear of it being monitored by their ex-partner. The clinic uses the *understand, investigate, advise* method discussed above via a remote consultation over the phone, similar to the procedures described in Tseng et al. [48]. In the course of the session, a number of challenges unfold for the technology consultant Taylor who volunteered to help Casey:

- Taylor asks Casey why they sought tech support. Casey provides a long history of their emotional and physical abuse, which takes time. While sharing this history, Casey becomes emotionally distraught, stating that they "feel hopeless" about escaping the abuser's reach.

- Casey describes problems that are technologically implausible, such as "every time I buy a new phone, he immediately hacks it". Casey describes how every phone exhibits behaviors that indicate it is "hacked", and that they've been avoiding use of their phones as a result. Casey's fear and frustration is palpable.
- Casey is unsatisfied with the account security checks that Taylor suggests. Casey insists that these are insufficient to catch their ex-partners' "hacking". Taylor tries to explain why it is useful to inspect account security, but Casey is frustrated, pointing out that they read many articles online about powerful hacking tools.
- The consultation goes past its scheduled end time. Taylor is disappointed and demoralized that they were unable to make meaningful progress in the session.

This vignette illustrates how traumatic stress reactions can color delivery of computer security interventions. Casey displays hopelessness, hypervigilance and avoidance towards technology, along with fear and frustration. Taylor must navigate this emotional landscape while interpreting Casey's descriptions of the technology abuse, unpicking where they align with the attack vectors that Taylor's expertise suggest are most plausible. Taylor is committed to trauma-informed service delivery, offering validation to Casey throughout the appointment. Nonetheless, Taylor worries that this validation is contributing to Casey's fears, and believes that Casey would benefit from professional counseling to cope with the emotional toll of the abuse.

Open questions. Our experience working with IPV survivors, as captured by the example above, suggests that we have more to learn about how traumatic stress reactions impact security interventions. Yet as discussed in the last section, beyond experience-informed anecdotes, no structured investigation has been conducted into whether current intervention designs and consultant training practices are sufficiently addressing the needs of clients experiencing traumatic stress reactions during sessions. In response, three key research questions guide the studies we introduce below:

(1) What challenges related to traumatic stress reactions do consultants encounter during sessions with clients?

(2) Are there patterns that capture how traumatic stress reactions interact with technology-enabled abuse that may inform best practice for security interventions?

(3) Are existing trauma-informed care practices used by, e.g., mental health professionals applicable to computer security interventions? If so, which ones, and how should they be integrated?

To answer these questions, we use a multi-part study design that builds from existing literature on trauma-informed practices in computing [12] and interdisciplinary work on traumatic stress reactions [25,33]. The first phase of the study entailed semi-structured interviews with technology consultants volunteering or working at computer security clinics in a direct service role. The second phase engaged subject matter experts in analysis of transcripts from a computer-security clinic documenting consultant-client interactions. Subsequent sections of this paper detail the specific methodology for each phase of the study.

Ethics. Drawing on best practices for conducting research with at-risk populations [4], we did not directly recruit survivors into this study as we had access to pre-existing data sources that produced a rich dataset pertaining to survivors' experiences accessing computer security clinic services. The data was collected under an IRB-approved study — survivors (clinic clients) opted into participation and received service regardless of research participation.

Additionally, this study does not include clinical diagnoses of clients. Despite involving subject matter experts in mental health in the study design and analysis, a diagnosis requires direct interaction between a client and a mental health professional, which this study does not entail. The SMEs identify patterns of traumatic stress reactions, but do not provide specific clinical diagnoses.

Lastly, we recognize the sensitivity of studying client-consultant interactions for both parties involved. Though such studies are necessary for advancing best practices, we view consultants as contributing emotionally-taxing labor under the best guidance available at the time, and take care to avoid reproducing their interactions in a disparaging light.

Positionality. Collectively, the authorship team has over 50 years of experience providing direct services to thousands of IPV survivors. The second, third, and fourth authors are SMEs in mental health, each being Master's level licensed clinicians with social work degrees who specialize in working with clients experiencing tech abuse. The remaining authors all have extensive experience providing direct services to survivors, operating technology abuse clinics, and conducting research on IPV and digital safety.

Our analytical lenses draw on anti-oppression frameworks that recognize how survivors are impacted by intersectional social and political identities [32]. These frameworks prioritize survivors' agency in navigating trauma. Our experiences and analytical lenses informed all aspects of this study, including our methodological choices to rely on pre-existing data and to mitigate unnecessary exposure of the research team to traumatic content. Throughout all phases of the study, we engaged in a reflexive practice, regularly discussing questions of ethics and bias, including our professional interest in the study recommendations.

Clinic	Locale	# Consultants Study	 Total	Host Site	Modality
MTC	Madison	2	4	UW-Madison	in-person
CETA	NYC	7	25	Cornell Tech	audio call
TECCC	Seattle	2	4	DV Service	video call

Figure 1: Breakdown of consultant participation by clinic.

4 Mapping Consultant Experiences

We start with an exploratory study with tech consultants at tech abuse clinics. We chose to begin by interviewing consultants to identify gaps in current trauma-informed training that have deleterious effects on computer security interventions, and to develop an initial mapping of how traumatic stress manifests during client-consultant interactions.

4.1 Methodology

Recruitment. We recruited 11 technology consultants for semi-structured interviews from three computer security clinics: the Madison Tech Clinic (MTC), the Clinic to End Tech Abuse (CETA) in New York City (NYC), and the Technology Enabled Coercive Control Clinic (TECCC) in Seattle. Figure 1 summarizes the number of participants from each clinic and the total number of consultants affiliated with each clinic at the time of the study in Spring of 2023.

Consultants from MTC and TECCC live and work in the same geographic area as the clinic, while consultants from CETA engage in remote consultations from their home locations across the US, Canada, and Europe. Consultants were eligible to participate in the study if they had participated in at least two or more client sessions in the six months prior to the interview. Because of the smaller sizes of MTC and TECCC, all eligible and willing participants were interviewed. At CETA, solicitation ceased at saturation, when interviews became repetitive.

Supervisors at each clinic helped determine eligibility, and eligible consultants were contacted by either the first or last author with an invitation to participate in a Zoom-conducted interview. Potential participants were informed that declining would not impact their relationship with either the host clinic or its affiliate partners. No compensation was offered for participation. We received IRB approval for this study.

Analysis. Interview questions focused on the challenges that arose during consultant-client interactions (e.g.: *How well did trauma-informed care training align with your in-session experiences? Are there situations that you feel training did not prepare you for?*). All participants consented to audio recording, and recordings were transcribed and anonymized by the interviewer before analysis.

The first and last authors used reflexive thematic analysis to identify common themes across the interview data, following the six-phase process outlined by Braun and Clarke [7]. Consistent with our study design that incorporates existing work in trauma-informed care, we used a hybrid approach of deductive and inductive analysis [24], beginning with codes that represented anticipated themes, and then modifying the codebook (available in Appendix B) as new codes emerged. This resulted in 5 parent codes and 24 additional subcodes. For example, the parent code *consultant strategies* included subcodes such as *validate client* or *try to set expectations*.

Four themes were identified that described challenges related to mental health and a need for additional support. These four themes, which we call challenges, were consistent across participants from all three clinic sites. To help preserve consultant anonymity, we label consultant quotes as C1–C11, rather than identifying the clinic with which a consultant is associated. Below, we italicize direct quotes, which may be lightly edited to avoid identifiability without changing meaning.

In what follows, we detail four challenges (labeled CH1–CH4 in the summary table in Figure 2) regarding client-consultant interactions and how established trauma-informed care practices fall short in supporting technology consultants' direct-service work with IPV survivors.

4.2 Findings

Challenge 1: Managing time for security inventions. Many clients do not delineate between tech abuse and other forms of abuse, in part because tech abuse can affect many different areas of a client's life. Thus, when clients are asked to describe their technology concerns, they often share it in the context of longer narratives. During interviews, consultants explained that they struggle to maintain a balance between making space for clients to process their experiences, while also adequately delivering security interventions in the constrained amount of time available for a session.

Consultants described a pattern in which they ask clients general questions about their technology concerns at the beginning of the session, and clients *"start expressing everything they've been through. Sometimes it's overwhelming"* (C1).

Drawing on their training, tech consultants recognized that clients often have few spaces to disclose their experiences of tech abuse, and many clients understandably do not delineate tech abuse from other forms of abuse. Consultants also pointed out that the non-technical information and abuse history may offer valuable insight to decipher technology abuse, making this overlap diagnostically relevant. For example, a client might recall an opportunity the abuser had to access their device during a memorable incident of physical abuse, or share who owned certain accounts in the context of detailing a pattern of financial abuse.

Yet, offering unbounded time for therapeutic processing at the possible cost of service delivery was a frequent point of tension for consultants. While validation was an important part of the service, consultants worried that an overempha-

Label	Finding
	Challenges Identified in Consultant Interviews (§4)
CH1	Consultants struggle to understand tech abuse without enabling potentially harmful or time-consuming abuse narratives.
CH2	Clients may have unrealistic expectations for technical solutions, leading to frustration or desperation.
CH3	Fears about technology are often misplaced, but countering such fears seems anti-thetical to trauma-informed training.
CH4	Consultants are unsure if or how to ethically end services, especially when tech abuse is indistinguishable from paranoia.
	Patterns Identified in Transcript Analysis (§5)
TP1	Clients describe tech abuse with uninterrupted narratives, potentially retraumatizing clients.
TP2	Security and privacy diagnostic processes may be seen as threatening to clients due to historical systems trauma.
TP3	Pre-conceived theories about tech abuse may be protective, and clients may not be ready to accept new information.
TP4	Difficulty managing disparate tech concerns contributes to distress near end of session–the "doorknob" problem.
TP5	Consultants struggle to deflect non-technical concerns or articulate technical limitations, tending to overavailability.
	Subject Matter Expert-Advised Care Practices (§6)
CP1	Refocus clients to tech concerns by compassionately interrupting or using validation as a pivot point.
CP2	Be transparent about security and privacy diagnostic procedures to ease fears and build trust.
CP3	Counter existing beliefs by validating experiences (not explanation), then helping re-interpret tech phenomena.
CP4	Scope technical concerns explicitly early on, including prioritizing highest-risk concerns.
CP5	Have and enforce boundaries on the service, couched in organizational limits, including an exit strategy.

Figure 2: A summary of our findings. Challenges (CH) were identified in tech consultant interviews (Section 4). Patterns (TP) of traumatic stress reactions were extracted from session transcripts (Section 5). Care practices (CP) (Section 6) were offered by subject matter experts (SMEs) in mental health who also helped identify transcript patterns.

sis on validation could mean *"sometimes we're not actually carrying out any security checks"* (C5).

Consultants also explained that clients may become increasingly distressed while sharing their abuse history, and consultants were unsure *"whether to let them continue talking and get more emotional or whether to stop them"* (C8). As one consultant neatly captured, unchecked story-telling could hinder delivery of security interventions:

> *Some of this is helpful. Some of this is not. All of it is taking up some time. How much is appropriate? Am I doing [clients] a disservice by just letting [them] continue talking?* (C10)

While several consultants found *"interrupting clients in the kindest way possible"* (C6) to be useful, consultants generally expressed reluctance to interrupt clients. Reasons cited for their hesitancy to interrupt included not knowing how to effectively interrupt, concern that interrupting would harm their rapport with the client, or that interrupting seemed incompatible with empathetic service delivery.

Challenge 2: Communicating technical limits. several reasons why they find it difficult to manage client expectations about their ability to address tech concerns. First, tech abuse in particular can extend abusers' ability to cause harm over long distances and/or time, increasing the sense of hopelessness and inescapability associated with technology abuse in particular. As one consultant noted, *"Sometimes the crisis scenario has been going on for I don't know how long. [A session] could go on for hours"* (C11).

Second, tech clinics are not equipped to help with every facet of tech abuse, some of which may require advanced diagnostic tools (e.g., suspected use of sophisticated spyware) and some of which may be better handled by other systems (e.g., legal injunctions against harassment). As a consequence of these two factors, clients may arrive at the session with unrealistic hopes for what the consultant may be able to do in a time and resource-constrained setting.

Clients may respond to these service limitations with a variety of traumatic stress reactions, often near the end of the session. One common reaction reported by consultants was frustration or even anger upon realizing that the security interventions at the clinic's disposal were insufficient for the client's needs. This ranged from clients expressing that the security interventions were too elementary for what they believed they needed, to the less common extreme of clients making (unfulfilled) threats to take legal action against the clinic.

Another common reaction that consultants cited was desperation for additional service. Clients were sometimes convinced that additional sessions might yield new information, even when consultants explain that they have no additional help to offer. As one consultant described,

> *After we say we haven't really found anything...they'll come back two or three months later and it's the same exact concerns. But then it's like, how do you set those boundaries? And when?* (C9)

Tseng et al similarly surfaced the difficulty in finding natural endpoints for service [48, 49]. Our study finds that this is not limited only to longer-term care models, and this challenge manifests across clinics with different service models.

Consultants in short-term service models also experience difficulty with time boundaries during a single session and pressure to continuously extend the depth and complexity of security interventions that they offer. One consultant summed up the predicament, stating: *"It's really hard to say no, because this is someone who's asking for your help and you do have the expertise to help them"* (C8).

Challenge 3: Unhealthy validation of technical fears. Clients often enter sessions with misunderstandings regarding the ease with which technology can be "hacked". This includes *"clients believing that normally functioning technology is being maliciously used against them"* (C6), such as unsubstantiated fears that phone calls are being monitored.

As one consultant noted, these misunderstandings are exacerbated by social attitudes towards cybersecurity, saying, *"Hollywood and tech companies keep people wondering about what is and isn't possible. For survivors, that leads to confusion"* (C4). Multiple consultants acknowledged that some client's fears might sound outlandish on face, but saw those fears as reasonable given the abuse, disinformation, and the abstruseness of many technology interfaces.

Tech consultant are therefore often required to counter such (mis)beliefs. However, this creates tension with a core tenet of trauma-informed care: *validation*, or the practice of explicitly affirming the worthiness of a survivor-client's feelings and experiences. Validation is heavily emphasized in consultant IPV training, in part because research confirms that survivors' valid technology concerns are particularly likely to be dismissed or minimized by people in positions of power (e.g., law enforcement, judicial officers) [52].

Consultants considered validation a crucial part of their practice. Sensitive to the fact that many clients *"might not have folks that believe them"* (C7) outside of the consultation, consultants observed that from their position as tech experts *"validating their concern and just listening to them...relieves their anxiety"* (C9). Aiming to counteract the minimization and dismissal that clients may have encountered elsewhere, consultants explain that they *"prioritize making [clients] feel heard and that they are not crazy because it's something people hear so often"* (C8).

Yet, consultants also express worry that for some clients, blanket validation could be unhealthy. When tech fears are not based in technical realities, validating that fear *"could be dangerous because if nothing is happening, it might make them more paranoid"* (C8). Though sympathetic to the client's confusion, consultants explained that they *"struggle to navigate validating feelings, but not necessarily technical concerns when there's no technical evidence"* (C5).

This was particularly thorny in the less common scenario that the client held more extreme beliefs. While quick to note this was not the dominant scenario they encountered, one consultant nevertheless explained that when working with clients whose beliefs included conspiratorial elements, *"you almost feel like you're validating someone's experience in ways that are unhelpful in the long run"* (C6).

In summary, the trauma-informed practice of validation becomes non-trivially complicated when navigating the ambiguity resulting from attempts to diagnose security and privacy risks with the limited set of tools available to tech clinics. As one consultant asked: *"What is healthy validation and what is not? It's not like there is a right answer, is there?"* (C11).

Challenge 4: Consultants lack an exit strategy. Across the interviews, consultants were reluctant to discuss encountering serious mental health issues. Participants repeatedly emphasized that serious mental health issues were not representative of the clients they typically work with and feared contributing to the systematic dismissal, stigmatization, and invalidation that many survivors already face.

Complicating this, consultants pointed out that they lacked a full set of diagnostic tools and computer security training to distinguish between a mental health crisis or high-risk, edge-cases of sophisticated technology abuse. One consultant described the precarity of working with clients whose concerns fell in this gray area:

> *I'm not about to diagnose anyone with anything, but some clients go very deep down the rabbit hole with their technology. And something like a configuration file on their Android phone, they might think that's spyware. Or they might think that there's something going on that, from a technologist's standpoint, isn't—I don't want to say it's not possible, because I don't know if it's possible.* (C7)

Though the use of sophisticated nation-state level spyware (e.g., NSO Pegasus [34]) against civilian targets is a well-documented occurrence, the current consensus among experts is that such sophisticated attacks would be rarely encountered in IPV, with less sophisticated abuse tools the empirically more relevant threat [2, 10, 38]. Consultants at IPV clinics are therefore mostly not equipped with training or tools that might help rule out use of more sophisticated attack tools, which, in turn, would aid in differentiating such threats from a client's conspiratorial or delusional beliefs.

Consultants question whether they should end service all together when they recognize that the client's beliefs or emotional state are beyond what the clinic is equipped to disambiguate or otherwise safely handle. And, if they ultimately believe this the best course of action, consultants were unsure how to do so:

> *The client was, you know crying, running from one room to another...just a very chaotic scene. [I had] to cut off the conversation, because it was not good for me and I doubt it was good for them. When someone is in more of a crisis state, there's a shared*

> *intensity to it. So I feel that stress, because I want to do things ethically and responsibly.* (C11)

Other consultants, often those who self-identified as being highly-experienced, shared similar anecdotes. In some cases, clients had technical issues the consultant was capable of addressing, but the client struggled with emotional regulation enough that the consultant could not identify or deliver a security intervention. In others, the client had severe issues with reality testing, such as a high degree of paranoia or conspiratorial thinking, that either lacked technical plausibility or that the consultant lacked the tools to disambiguate.

In these situations, consultants reported doubt that the services offered by the clinic were beneficial for the client or indeed whether they were appropriately equipped to safely provide service without direct oversight from professionally-trained mental health experts.

While none of the clinics operate with the resources or training to provide this form of support, the inherent nature of the service means that consultants must navigate the possibility of encountering such clients. Organizational level practices, such as robust screening processes at intake, can mitigate the likelihood of these situations occurring, but consultants still need ethical exit strategies to facilitate hand-off from certain consultations to more appropriately equipped services.

5 Analyzing Transcripts of Clinic Sessions

Our study with consultants surfaced common challenges related to traumatic stress reactions across all three clinics. These challenges indicate that delivery of security interventions is meaningfully affected by the impacts of traumatic stress, and that current trauma-informed care training is insufficient to fully address these complexities. Seeking a deeper understanding of the role of traumatic stress in security interventions, we turn to a more granular investigation by analyzing session transcripts to identify patterns in how stress reactions arise.

5.1 Methodology

CETA has an ongoing IRB-approved research study on technology abuse. At the start of a client session, the client is consented into research participation and, if so, for permission to audio record sessions. Clients are informed that they will receive the same service from the clinic whether or not they consent, and client support proceeds the same regardless of research participation. Session transcripts offer unique insight into the dynamics of client-consultant sessions, while also obviating the need to conduct a separate research study directly with survivors which could, itself, be a source of burden or even trauma for them (see [4]).

At the time of the study, the CETA transcript database contained 218 anonymized transcripts from phone-based appointments with 161 different clients. All 18 transcripts considered below involved distinct clients. CETA does not collect or retain demographic information about individual clients represented in the data, and the nature of our study does not support demographic-level analyses. However, CETA serves a diverse, minority-majority population: 78% of clients seeking IPV services in New York City are female, with 59% being foreign born, 66% being non-white, and 5–8% identifying as LGBTQ+.

To provide clinical insight to our analysis, the subject matter experts (SMEs) among our authorship team (see Section 3) participated in coding the transcripts and in augmenting the transcripts with annotations.

Coding. Lacking prior validated techniques for prescreening transcripts for inclusion through, e.g., keyword search, we randomly sampled transcripts. SMEs drew on their professional expertise to designate an initial set of codes for analyzing the transcripts that were indicative of traumatic stress reactions. The first author and an SME then refined the codebook over an initial sample of six transcripts, meeting regularly to confer and discuss newly emerging codes [24]. This resulted in a codebook with a total of 23 codes, available in the Appendix B: 13 codes representing traumatic stress reactions and 10 codes describing consultant demeanor.

Examples of codes representing traumatic stress reactions include: *information dumping*, *physical symptoms*, and *anger, frustration, and resentment*. The authorship team then used this codebook to analyze an additional 12 randomly selected transcripts, working in pairs that included an SME. We identified saturation as the point when no new codes were being generated and all identified codes had been applied with expected frequency, and ended sampling. By expected frequency, we mean that traumatic stress reactions appeared in the data at what SMEs found consistent with professional experience, with codes indicating common reactions like *hypervigilance* appearing over 80 times but rarer, more serious reactions like *hallucinations, delusions, and psychosis* appeared fewer than 25 times. Ultimately, 18 transcripts were analyzed for the study. Below, references to transcripts are labeled T1–T18.

Annotations. During the coding process, SMEs noted that traumatic stress reactions are often not explicit in the text of an interaction. For example, an interaction in which a client repeatedly avoided a question from a consultant was coded as a potential marker for anxiety, even though the client did not explicitly state "I feel anxious".

To capture these nuances, we introduced a protocol for annotating transcripts after coding them. In keeping with our ethical commitment to reduce the emotional burdens and time commitments placed on the SMEs (who work as full-time practitioners with survivors), our annotation protocol incorporated a collaborative focus group approach in which the SMEs provided clinical analysis of the transcripts during structured sessions.

We held eight focus groups over Zoom attended by one or more SMEs, in addition to a non-SME facilitator. Each focus group analyzed 1–2 transcripts. The facilitator started each session by providing a brief overview of the interactions in the transcript. The facilitator then instructed the SMEs to read segments that had been previously coded, after which the SMEs were prompted with questions such as: *Why did this interaction suggest hypervigilance? What might have caused this reaction?* This analysis was captured by the facilitator via annotations of the transcript segment.

As part of our ethical strategy to reduce vicarious trauma, we were reflective about identifying saturation points as soon as possible: focus groups were ended when all codes had been encountered and SMEs explicitly noted that their annotations and analysis were repetitive. This process resulted in annotations of nine transcripts across eight sessions.

Analysis. The coded and annotated transcripts formed the basis for our analysis. When reflecting on potential themes, the first and last authors considered the transcript segment, the code, and the annotations provided by the SMEs together. Other than the inclusion of annotations, the first and last authors used a similar analysis process in developing themes as in Section 4.1. We identified five patterns and mitigation strategies, which we outline below.

To provide additional context, we note whether these patterns tend to occur during a specific stage in the *understand-investigate-advise* protocol. An overview of how these patterns relate to each stage in the consultation protocol as well as their relationship with challenges identified by consultants is presented in Figure 3.

5.2 Findings

We start by discussing five patterns identified during our transcript review, including the SME-informed explanations of why those patterns might occur. We summarize these patterns, labeled as TP1–TP5, in Table 2. We discuss practical tools to help consultants navigate these patterns in Section 6.

In what follows, we ground our findings with examples from session transcripts of client-consultant interactions. In order to protect the privacy of clients and consultants, we primarily use composite examples that represent common interactions across multiple sessions. We include direct quotes only when the speaker would not be recognizable by quote.

Pattern 1: Uninterrupted narratives. Consistent with consultant experiences in CH1, SMEs identified a pattern in which open-ended questions about the client's technology concerns were answered by detailed, non-linear narratives of their abuse history. This was especially common during the early, exploratory phase of the session, where a session transcript might entail upwards of ten minutes of clients continuously speaking about both technical and non-technical concerns. During these long narratives, consultants typically listened without speaking or occasionally offered a validating response of "I see" or "I'm sorry that happened."

Sharing these stories without interruption and receiving validation can help establish needed rapport, especially early on. However, SMEs raised several potential pitfalls. While an obvious drawback concerns time management, others were specific to traumatic stress reactions. Namely, revisiting potentially traumatic experiences at length and in depth can be *retraumatizing*, engendering reactive states for survivors that can hinder their ability to effectively and productively engage with technology support services [19].

Shorter but emotionally charged client narratives also occurred during walkthroughs of security interventions, especially when clients found something confusing or unfamiliar. If clients had already shared longer narratives early on (such as a story about how the abuse had affected their children), they would often reference those narratives again later: *"It just sucks for my kids, you know?"* (T4). Indeed, one client alluded to this process of retraumatization directly, saying: *"It's all triggering. It reminds me of how chaotic these moments were when I was receiving this stuff"* (T16).

This apparent switching between the concrete task at hand and recounting experiential anecdotes might also have long-term impacts. As tech consultants are unable to provide long-term therapeutic support, negative or unsatisfying experiences with sharing sensitive stories during the clinic session might even discourage the client from sharing those experiences in more appropriate professional settings. Similarly, SMEs pointed out that if clients did not understand that they were not obligated to disclose weighty, sensitive information in order to receive help, this might discourage clients who were not ready to make such disclosures from seeking support for technology or security intervention services in the future [23].

Pattern 2: Identifying security concerns. Another pattern of traumatic-stress reactions surfaced during the diagnostic, investigative portions of sessions. As previously noted, clients often arrive with vague or technically imprecise descriptions of their experiences, stating that their phone or device was 'hacked', 'cloned', or being 'constantly monitored'. To help pinpoint explanations, consultants embark on a series of questions intended to differentiate possible security risks, a process which could quickly become tense.

This most often manifested as evasiveness or frustration when asked diagnostic questions without context. For example, one client avoided answering whether the abusive party had been able to physically handle the device (T2), possibly wary that her concerns might be dismissed should she answer no. In another, a client repeatedly dodged a direct question about whether unusual behavior had persisted after switching devices by repeating what they had heard from a friend (T13).

Protocol Stage	Goals	Identified Challenges (CH)		Identified Patterns (TP)	
Understand	active listening to understand client issues, open-ended exploratory questions, mapping of potential threats	time management information dumping	CH1	retraumatization information dumping	TP1
Investigate	manually check security and privacy configurations, identify potential safety risks, document suspicious settings	unrealistic expectations ambiguous outcomes	CH2 CH3	systems trauma protective beliefs	TP2 TP3
Advise	devise likely explanations, provide safety information and education, suggest tools or strategies for improving safety	service overusage exiting unsafe situations	CH2 CH4	"doorknob" phenomenon overavailability	TP4 TP5

Figure 3: A description of the understand-investigate-advise protocol, annotated with where consultant-identified *challenges* (CH) and transcript-identified *patterns* (TP) most commonly surface, using the labels from Figure 2.

Consultants, sensing the fragility of the moment, would often pause diagnostic process to try and re-establish rapport.

SMEs explained that diagnostic questions can be particularly loaded for clients whose past experiences with "the system" have taught them that failing to fit neatly into apparently arbitrary criteria might result in their concerns being wholesale dismissed. This is possible for all survivors, but especially likely for marginalized populations such as LGBTQ+ and/or immigrant survivors. Such experiences are known as *systems trauma* [9]. As consultants noted and as prior research supports, survivors are especially likely to have invalidating experiences when seeking help for technology abuse [52].

Second, clients might not be familiar with the diagnostic protocols that consultants use to help tease out and organize tech abuse concerns. Consequently, when asked diagnostic questions without an explanation of why that question is necessary, clients may be skeptical of how their answers will affect the service they receive or whether the question itself is a sign of doubt.

Pattern 3: Countering existing beliefs. The delicacy of navigating exchanges in which clients disclosed fears which were not technically plausible was frequently observed. As consultants interviews also suggested in CH3, clients often arrive at the clinic with an explanation or theory in mind as to how the tech abuse is being conducted. Notably, prior research has confirmed that abusers tend to overstate their technical abilities as a control tactic, causing survivors to believe that the technical explanation for their experiences is highly sophisticated [14]. Thus, when consultants attempted to push back on this belief, subsequent interaction between clients and consultants were fraught.

This tension was observed in several transcripts (T2, T5, T15, T16). While individual circumstances are too identifying for detailed description, they all centered around a belief that the abuser had abilities allowing them to totally and immediately monitor or manipulate the client's electronic devices. The SMEs recognized the predicament in steering the session: if consultants pushed too hard, they risked the client shutting down or becoming unreceptive to new information. However, blanket validation could be interpreted as endorsing misconceptions about the technical capabilities of abusers.

In such scenarios, SMEs explained that clients often hold these beliefs as a form of protection against danger or difficult emotions, thus it may feel threatening for clients to release those protective beliefs, especially in the moment. Nonetheless, they pointed out that the safety information provided by consultants could be valuable for managing traumatic stress reactions in the long-term.

For example, *hypervigilance* is a common traumatic stress reaction in which survivors are highly sensitive to warning signs of danger or abuse. This adaptation, while protective during on-going abuse, can become problematic when benign events are misidentified as threats [41]. Thus, technologists are positioned to supply clients with accurate information about security and privacy risks that, accompanied by therapeutic treatments, could potentially aid in managing anxiety, hypervigilance, and other traumatic-stress reactions related to the technology abuse.

Pattern 4: The "doorknob" phenomenon. The well-documented tendency of tech abuse being deployed in complex, disparate methods for even a single client was evident in the transcripts. Clients often arrived wanting to understand the security and privacy risks of each of many devices. In part owing to the cognitive impact of traumatic stress and the obfuscated nature of tech abuse, clients may struggle to organize those concerns into manageable task. Thus, tech consultants faced difficulty in scoping sessions for what could reasonably be accomplished in the allotted time.

SMEs noted that sessions lacked clear boundaries around length, ranging from 60–90 minutes. Additionally, consultants sometimes struggled to manage the pace of the appointment when clients shared many disparate concerns. This contributed to a familiar pattern of distress known as the "doorknob" phenomenon [22] near the end of sessions: when clients ask a rapid series of questions or raise new, seemingly urgent issues at the end of an appointment, just as the provider reaches for the door to exit the office.

In one sampled transcript, a consultant began summarizing completed and outstanding tasks, at which point the client began a block of questions related to hardware security, an upcoming court date, utility plans, and online blocking mechanisms (T4). In other end-of-session examples, clients apologized for wasting the consultant's time (T9), and in a more extreme example, explicitly alluded to panic when the consultant alluded to wrapping up (T5).

Pattern 5: Out-of-scope concerns The overwhelming majority of transcripts depicted momentary traumatic stress reactions occurring in the context of a session that otherwise consisted of security interventions and rather dry discussion of technical details. However, as consultants described in CH5, in two transcripts (T5, T15) in which the each client showed severe signs of difficulty distinguishing reality from conspiracy or paranoia, and a third (T9) demonstrated a fundamental mismatch vis-a-vis the client's needs and the clinic's scope.

More commonly, clients sometimes disclose urgent needs that were beyond the scope of the clinic. This included tech-based concerns, like home visits to search for tracking devices or collecting evidence for a court case. It also included non-technical concerns such as difficulty affording food or basic utilities or needing medical care. In all cases, consultants offered compassionate and empathetic responses, but frequently struggled to articulate limits on what the service was capable of providing.

In general, we noted a tendency towards *overavailability*, observing that consultants rarely explicitly set boundaries around ending service with a client. Consultants almost always closed sessions by asking clients if they would like another appointment, even if they had done a thorough job addressing all concerns during the session.

This is consistent with the difficulty in drawing boundaries reported by consultants in interviews and in Tseng et al [49]. SMEs were able to provide additional context on why ending service with intentionality was consistent with compassionate care. If the client was navigating a fundamental mistrust of technology, the client could likely find fodder to discuss with the consultant indefinitely, setting them up for infinite appointments and increasing the likelihood of an abrupt cutoff.

Tech abuse, in particular, can manifest in a manner that lacks the natural endpoint found in, e.g. housing or job placement. Organizational processes (screening, appointment caps) can provide structure that encourages or builds in service limits. However, even with organizational support, our findings here reinforce a need to equip tech consultants with the ability to articulate and enforce service limitations.

6 Care Practices for Security Interventions

Towards identifying opportunities for practical improvements concurrently with problems, we also asked our SMEs to share strategies for the challenges and patterns uncovered in consultant interviews and transcript analysis. During focus groups, SMEs recommended five targeted strategies for consultants to use during client sessions. Following the work of Tseng et al. [49], we term these strategies *care practices*.

Practice #1: Refocus the conversation. Consultants were understandably reluctant to interrupt clients, and viewed active listening as foundational to trauma-informed care. While SMEs saw this benefit, they explained that compassionate, trauma-informed care included helping survivors be intentional in when and whom they shared emotionally-charged and potentially re-traumatizing stories. While avoiding re-traumatization entirely is unrealistic, SMEs suggested two methods for gently refocusing clients when experiential sharing began to dominate the session.

First, SMEs encouraged consultants to interrupt or "pause" clients when they were speaking at length about tangentially related subjects. SMEs pointed to a consultant who positively modeled this with a client. Having already discussed multiple devices, the consultant stopped the client from revisiting concerns about yet another, since-abandoned device by saying: *"Taking it one step at a time, right? Let's focus on securing the phone that you have with you."* (T13) Similarly, another consultant diverted a client mid-narrative by saying: *"I'm just going to focus us on the task at hand, the Internet connection."* (T9). As SMEs noted, a gentle interruption *was* compassionate when it helped clients meet their goals for the session or de-escalated trauma stress reactions.

Second, SMEs noted that validating a client's experiences can serve as a method for redirecting the conversation toward a relevant security intervention. By acknowledging the worry that the client is expressing about a security concern or the abuse more broadly, the consultant can refocus the client by explaining how the clinic session may address that worry. A consultant modeled this strategy when a client became distressed while discussing circumstances around interactions with law enforcement. The consultant replied:

> *I'm so sorry to hear that. That sounds really scary but I'm glad you shared that so we know to document any potential evidence we see today.* (T8)

Validating statements such as this tactfully acknowledges the client's distress, but simultaneously refocus the session back to the security intervention. Such redirection tactics are particularly useful for tech consultants, who are navigating concrete and technical solutions that require attention and focus against an emotionally charged backdrop.

Practice #2: Demystify tech through transparency. To minimize the likelihood of recalling past traumatic or invalidating experiences with "the system", SMEs suggested demystifying the tech diagnostic process by being transparent about what the consultant is doing and why, at each step. For example, consultants can be upfront about having a list of diagnostic questions, and reassure clients that their answers to those questions should help narrow down possible explanations. One consultant modeled this, saying *"I want to understand what's going on a little better and just like going to the doctor, I'm going to have questions"* (T13).

As another example, consultants can acknowledge that they will be moving through a series of security interventions, some or all of which might not yield any new information. One consultant demonstrated this when a client became frustrated with a suggested security intervention, saying

> *Sorry if anything we do is repetitive. We take your safety really seriously, so we're not going to skip anything unless you tell us to.* (T4)

Slupska et al [45] identify *demystification* of technology as an "interwined emotional and technical support practice" and our findings are consistent with this description; however, we find that when clients are receiving dedicated tech services, the entire session or service itself may be viewed as an opaque tech phenomenon. Here, demystification is a necessary component of building trust and rapport for the service as a whole.

Practice #3: Validate experiences, not tech explanations. As SMEs warned, a client who enters with a preconceived explanation about the nature of their tech abuse may not be able to accept information that threatens the validity of that explanation. The SMEs recommended that consultants be aware of this, and offered a two-part strategy in which consultants first validate the client and then offer alternative explanations.

Crucially, practitioners recommended avoiding validation that engages directly with the misbelief itself. Instead, they provided several components of the client's experience to safely validate. This avoids seeming contradictions later on, while still signaling that the consultant is actually hearing the client, not reacting with a knee-jerk dismissal.

These components included the *disruptiveness of the distress*. For example, rather than affirming that the client's phone is "hacked", the consultant can instead affirm the logistical difficulty of *avoiding using your phone*. Additionally, consultants can use their credibility as technologist to *validate the complexity* of understanding how to secure a piece of technology, especially in the face of misinformation, and the client's labor in navigating that confusion.

When offering alternate explanations, SMEs again offered several tools. Some examples include transparency around the logical process that lead to that explanation, tools for testing theories in the future, and how to disengage if the client rejects the offered explanation.

Similarly, consultants can provide limited *psychoeducation* [6] for clients, explaining to clients the manipulation tactics that perpetrators often deploy in the context of tech abuse. Examples include the research-supported pattern of perpetrators overstating their technical abilities as a tool to instill fear in victims, exploiting, e.g., attempted log-in notifications as a communication mechanism, or the tendency of abusers to use one or two pieces of information to gain credibility when they falsely claim that they "see everything".

Practice #4: Set expectations for the session. Best practice encourages having firm boundaries around the length of an appointment. This is especially important given the far-ranging nature of tech abuse which lends itself to an overwhelming amount of ground to cover. Perhaps unintituively, how a session ends is largely influenced by how it begins. Thus, SMEs recommended engaging the client in explicitly establishing a timeline and agenda together early on, a practice which helps build rapport and manage expectations.

This includes beginning an appointment by noting the length of the appointment, and periodically incorporate time cues throughout the session. For example, half way through an appointment a consultant might state: *I think that within the 30 minutes we have, we would be able to walk-through the security of your email account.* As the SMEs explained, time cues can serve as an important grounding tactic for clients who may be experiencing traumatic stress reactions.

Similarly, the SMEs highlighted the importance of working with clients to identify their most pressing concerns (referred to as chief concerns by Havron et al. [30]) at the start of the appointment, in order to ensure their most urgent concerns aren't overlooked. Good prioritization, according to the SMEs, should recap a client's concerns, and encourage feedback on a plan for how and when they will be addressed. Within the context of tech abuse, this includes accounting for which technical concerns are having the deepest impact on the client's ability to function. For example, a consultant might say: *Of all your concerns, it sounds like the phone and email are your priority. We can focus on that today and discuss other concerns in a follow-up. Is that okay?*

This pacing approach removes responsibility from the client for maintaining the cognitive load of both task organization and time management, while still making sure the client's priorities are acknowledged and reflected by the session.

Practice #5: Set (and embrace) limits for the service. A single service provider is incapable of attending to all of a client's multi-faceted needs, and SMEs were cognizant of the pressure technology consultants might feel when clients brought up issues beyond the clinic's purview. Unfortunately, in the ever-shifting landscape of tech abuse, clients will inevitably have concerns both technical and non-technical that the service is not equipped to address.

Along with an agenda for the session itself, expectations for the limits of the service should also be set at the start of service. An initial session should frame the conversation as a means to understand *if* the clinic may help, not *how*. This framing builds an exit hatch into the session—if initial exploration reveals that the clinic cannot address the client's needs, they can refer back to the expectation set at the beginning.

In cases where clients explicitly raised non-technical issues or needs that would be best met by other services, such as the mental health impact of the tech abuse or financial difficulties, consultants can offer to echo those concerns back to the social worker who referred the client to the service. However, SMEs agreed that caution was needed in directly recommending therapy services. If unsolicited, such recommendations could be inappropriate or offensive.

Crucially, SMEs offered useful criteria for reframing the decision to end service, especially when encountering clients who raised technical concerns that could not be disambiguated from signs of paranoia by the clinic. Instead of focusing on plausibility of concerns, SMEs suggested that continued service instead be contingent on whether the consultant finds that they are able to gain *traction* in diagnosing tech issues and/or identifying a set of finite, actionable tasks within the clinic's purview. If the consultant finds that they are unable to understand the client's concerns or that the client's concerns shift too rapidly, as observed in a couple transcripts, this signified a lack of traction. This framing offered reasonable criteria to end service.

More broadly, this practice can also be viewed as asking consultants to set expectations for themselves and the service as a whole. Without internalizing these inherent limits, consultants may face overly high expectations concerning what they are able to accomplish in their role, increasing the risk of burnout or dissatisfaction. Conversely, understanding the organization's remit and staying firmly within that lane can be empowering for consultants. This is especially important for tech consultants, as our findings suggests that security and privacy services are particularly likely to encounter situations in which it is difficult to disambiguate serious mental health issues from low-probability but feasible security risks.

7 Embedding Care Practices into a Protocol

In this section, we demonstrate how the care practices described above could be embedded into the structure of security intervention delivery. We are inspired by the understand-investigate-advise (UIA) protocol which was introduced by Havron et al. [30] (discussed in Section 2). It embedded trauma-informed practices into its design: for example, it encouraged active listening as an initial stage, framed the consultant role as advisory rather than instructive, and incorporated hand-offs for professional safety planning.

However, as Figure 3 shows, certain traumatic stress reactions tend to occur during particular stages of the protocol, suggesting it would benefit from refinement. Thus, we propose an alternate protocol in Figure 4. New stages are highlighted in yellow. All stages incorporate one or more suggested care practices intended to alleviate the recurrent patterns of traumatic stress reactions documented in our study. We discuss each stage in order below, connecting it back to our example of Casey and Tyler from Section 3.

- **Orient.** Given the tendency for clients to arrive at tech clinics with outsized hopes, SMEs viewed setting expectations early as a crucial practice for tech consultants. Thus, we devote an initial stage to this practice. In the example of Casey and Tyler, Tyler could begin the session by acknowledging that the clinic has a limited set of tools that might not meet all or any of Casey's needs.
- **Understand.** In this stage, we find it most useful to utilize strategies that can pause the client or gently steer them away from sharing re-traumatizing information, as in CP1. Going back to our example, Tyler could stop Casey when Tyler notices Casey's emotional state escalating, by saying, for example, *"Casey, can I stop you for a moment? I'm happy to listen, but I have some questions that might be important to clarify first."*
- **Plan.** We insert a planning stage as a bridge between the more open-ended exploration of *understand* and the concrete tasks in *investigate*. This is a moment to acknowledge that the tools available to the clinic might have limited use, and to check whether the client would like to proceed. For example, Tyler can use this moment to tell Casey, *"We can start by ruling out some common causes, and talk about next steps based on what we find. How does that sound?"*
- **Investigate.** The investigation stage benefits greatly from transparency throughout the process (CP2). Having set expectations in prior stages means that although Casey might not feel the interventions are powerful enough for their situation, they are entering with an understanding of what to expect and why it might be beneficial. Continuing to explain the logic behind each check and its necessity maintains this rapport.
- **Advise.** Consultants demonstrated a strong capacity for compassionately dispensing safety information about technology. This practice can be strengthened with a specific understanding of how to validate experiences without validating explanations. For example, Tyler, having practiced this skill, might say *"I know how important securing this account is; based on the steps we took, we can rule out account compromise here."*
- **Wrap up.** We encourage firm endings via a "wrap up" stage. At this point, if Tyler has exhausted the available security interventions and Casey is still not satisfied with the lack of explanations, Tyler can fall back on the initial expectations set at the beginning, saying, *"I'm sorry that we didn't find an explanation, but I don't think more sessions would be fruitful."*

8 Discussion

This is an initial study examining how traumatic stress reactions affect computer security interventions. We recognize that in studying traumatic stress, we have highlighted significant negative impacts on both consultants and survivors during computer security interventions. Despite the neces-

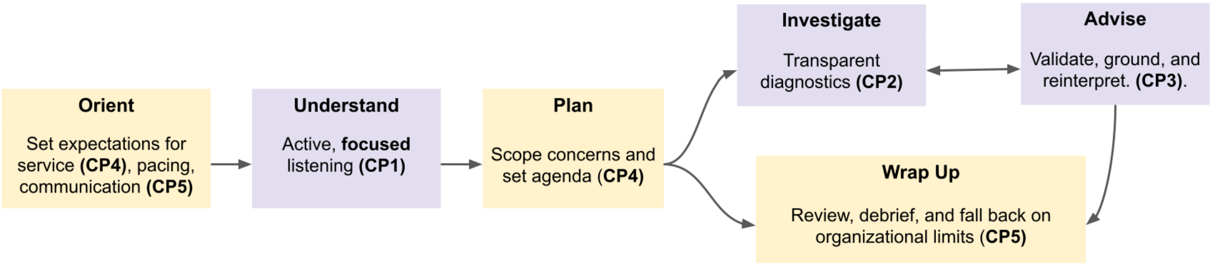
Orient
Set expectations for service (CP4), pacing, communication (CP5)
Understand
Active, focused listening (CP1)
Plan
Scope concerns and set agenda (CP4)
Investigate
Transparent diagnostics (CP2)
Advise
Validate, ground, and reinterpret. (CP3).
Wrap Up
Review, debrief, and fall back on organizational limits (CP5)

Figure 4: Diagrammatic summary of a new tech consultation protocol, based off UIA [30], labeled with practices from Figure 2.

sity of surfacing these pitfalls towards improving services, it is important to recognize the many positive effects of these services for both clients and consultants; we highlight these throughout below.

Returning to the questions that guided these studies (see Section 3), we began by asking what challenges related to traumatic stress reactions do technology consultants encounter during sessions with clients. We were especially interested in consultants' perspectives on why certain types of interactions were challenging, and their answers pinpointed specific, actionable gaps in trauma-informed training.

We also note that both studies demonstrate that consultants are engaging in emotionally intensive labor during sessions that may expose them to vicarious trauma. Elsewhere in interviews, consultants often described their work as rewarding and meaningful, and analysis of session transcripts overwhelmingly reinforced that consultants compassionately deliver useful safety information.

We anticipate that the findings of this study will validate consultant experiences by highlighting areas for necessary improvements to training. We hope future studies seeking to further understand how traumatic stress reactions affect computer security interventions will include specific focus on mitigation strategies for vicarious trauma.

In our second research question, we were interested in identifying patterns regarding how and when traumatic stress reactions occur during sessions. Resulting analysis allowed us to identify how traumatic stress reactions map on to the flow of a session. While our transcript study only drew from a single clinic, the interview component showed that consultants have difficulty navigating similar types of interactions across all sites, suggesting that these challenges follow patterns that are agnostic to location or modality (e.g., video call, phone call, or in-person). Thus, in addition to enhanced trauma-informed training, the results from this study also suggest that training focused on how traumatic-stress reactions present across the structure of a session may benefit consultants.

The challenges identified by consultants in Section 4 were supported by analyzing the transcripts in Section 5. Indeed, the additional analysis provided by the SMEs showed that subject matter expertise can identify new issues, such as the tensions during diagnostic questions in TP2. They can also provide useful context for reframing challenges, such as the potential for long narratives to not only create time pressure (CH1) but also to potentially retraumatize clients (TP1).

Our third research question aimed to identify potential strategies for mitigating traumatic stress reactions during clinic sessions. While SMEs suggested specific mitigation strategies, the consistent patterns that emerged from both studies suggest that re-structuring sessions at key moments where traumatic stress reactions tended to occur might be beneficial for both the clients and the consultants managing the sessions. Our proposed protocol builds on prior work [30] by identifying these critical moments and explicitly including steps to preemptively incorporate mitigation strategies.

Beyond advancing clinical computer security protocols, this work builds on literature spanning multiple disciplines. Most crucially, our findings position digital security and privacy workers as front-line service providers. Prior work has demonstrated intersections between at-risk populations and digital safety advocates, including journalists, activists, and refugees of war or natural disasters. While we focus on survivors of IPV, we view these studies as affirming the need for trauma-informed protocols similar to other roles such as public defenders, prosecutors, social workers, and health care providers when working with vulnerable populations writ large. We believe our study design, especially our approach to including mental health clinicians as subject matter experts, can inspire similar future work.

Future Work. As stated, we are interested in developing trauma-informed protocols for other at-risk populations besides IPV survivors such as those outlined above. We also see potential for additional studies using ethnography-inspired approaches that include mental health professionals observing sessions or examining other IPV contexts, such as temporality (e.g., during separation versus years after), or exposure to different types of abuse (e.g., image-based abuse, trafficking, identity theft).

Solutions offered here center on consultants, but we note a need for organizational-level practices, such as robust screening and intake processes and incorporating oversight from mental health professionals into high-risk sessions, and embedding these practices into training. More broadly, this work raises questions regarding the unique characteristics of traumatic stress reactions in relation to technology abuse. Our findings indicate that therapeutic treatments for stress reactions like hypervigilance may require input from security and privacy professionals, and future work may explore collaborative tool development for such treatments.

Limitations. This study focused on computer security interventions for survivors of IPV, and our results may not extend to security interventions in other contexts (e.g., other populations, general security customer support, etc.). However, our paper's methodological approach—combining semi-structured interviews of tech consultants, along with SME-assisted analysis of client-consultant interactions to develop new best practices—should be useful in future studies investigating other contexts such as those outlined above.

Related to the scoping limitations, while consultants identified common challenges consistent across all three sites, the transcripts used in this study were from a single clinic. Though this clinic serves a large, diverse population, minor differences in clinic protocol such as training or modality (e.g., remote, in-person) may not be accounted for. Similarly, our random sample of transcripts may have failed to capture nuances that depend on specific demographics or intersectionality, such as survivors marginalized by race or sexuality.

Finally, the sampled database only includes textual transcripts from sessions in which clients consented to research. Thus, nuances that might be available in audio recording, video recording, or in person observation can be lost. Likewise, trauma may play a role in motivating or deterring a client from consenting to participate in research, resulting in potential bias within our sample. Though our incremental sampling approach was designed to account for this, it is possible that clients experiencing certain types of traumatic stress reactions (e.g., hopelessness, hypervigilance) may be more or less likely to consent to research.

Acknowledgements

This work was partially supported by the NSF grant 2127309 for the CRA CIFellows 2021 Project, NSF grant 1916096, and a gift from J.P. Morgan Chase.

References

[1] Laken Gilbert Albrink. Trauma-informed legal advocacy. *Wake Forest JL & Pol'y*, 13:67, 2023.

[2] Majed Almansoori, Andrea Gallardo, Julio Poveda, Adil Ahmed, and Rahul Chatterjee. A global survey of android dual-use applications used in intimate partner surveillance. *Proceedings on Privacy Enhancing Technologies*, 2022.

[3] Rosanna Bellini, Emily Tseng, Nora McDonald, Rachel Greenstadt, Damon McCoy, Thomas Ristenpart, and Nicola Dell. "So-called privacy breeds evil" narrative justifications for intimate partner surveillance in online forums. *Proceedings of the ACM on Human-Computer Interaction*, 4(CSCW3), 2021.

[4] Rosanna Bellini, Emily Tseng, Noel Warford, Alaa Daffalla, Tara Matthews, Sunny Consolvo, Jill Palzkill Woelfer, Patrick Gage Kelley, Michelle L Mazurek, Dana Cuomo, et al. Sok: Safer digital-safety research involving at-risk users. In *IEEE Symposium on Security and Privacy (SP)*, 2024.

[5] Rasika Bhalerao, Vaughn Hamilton, Allison McDonald, Elissa M. Redmiles, and Angelika Strohmayer. Ethical Practices for Security Research with At-Risk Populations. In *2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*.

[6] Erica Bowen, Kate Walker, and Emma Holdsworth. Applying a strengths-based psychoeducational model of rehabilitation to the treatment of intimate partner violence. *International journal of offender therapy and comparative criminology*, 63(3):500–517, 2019.

[7] Virginia Braun and Victoria Clarke. *Thematic analysis.* American Psychological Association, 2012.

[8] Bradley A Campbell. Advancements in trauma-informed training and interviewing for law enforcement and prosecutors. In *Sexual assault kits and reforming the response to rape*, pages 315–326. Routledge, 2022.

[9] Center for Substance Abuse Treatment. *Trauma-Informed Care in Behavioral Health Services*. SAMHSA/CSAT Treatment Improvement Protocols. Substance Abuse and Mental Health Services Administration, Rockville, MD, USA, 2014.

[10] Rahul Chatterjee, Periwinkle Doerfler, Hadas Orgad, Sam Havron, Jackeline Palmer, Diana Freed, Karen Levy, Nicola Dell, Damon McCoy, and Thomas Ristenpart. The spyware used in intimate partner violence. In *IEEE Symposium on Security and Privacy (SP)*, 2018.

[11] Christine Chen, Nicola Dell, and Franziska Roesner. Computer security and privacy in the interactions between victim service providers and human trafficking survivors. In *Proceedings of the 28th USENIX Conference on Security Symposium*, 2019.

[12] Janet X Chen, Allison McDonald, Yixin Zou, Emily Tseng, Kevin A Roundy, Acar Tamersoy, Florian Schaub, Thomas Ristenpart, and Nicola Dell. Trauma-informed computing: Towards safer technology experiences for all. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, CHI '22.

[13] Dana Cuomo, Nicola Dell, Alana Ramjit, and Thomas Ristenpart. The technology abuse clinic toolkit,

2023. https://www.techabuseclinics.org/the-toolkit.

[14] Dana Cuomo and Natalie Dolci. New tools, old abuse: Technology-enabled coercive control (tecc). *Geoforum*, 126:224–232, 2021.

[15] Dana Cuomo and Natalie Dolci. The TECC Clinic: An innovative resource for mitigating technology-enabled coercive control. *Women's Studies International Forum*, 92:102596, May 2022.

[16] Alaa Daffalla, Marina Bohuk, Nicola Dell, Rosanna Bellini, and Thomas Ristenpart. Account security interfaces: important, unintuitive, and untrustworthy. In *32nd USENIX Security Symposium*, 2023.

[17] Gina Dillon, Rafat Hussain, Deborah Loxton, and Saifur Rahman. Mental and physical health and intimate partner violence against women: A review of the literature. *International journal of family medicine*, 2013.

[18] Jill P Dimond, Casey Fiesler, and Amy S Bruckman. Domestic violence and information communication technologies. *Interacting with computers*, 23(5):413–421, 2011.

[19] Denise E Elliott, Paula Bjelajac, Roger D Fallot, Laurie S Markoff, and Beth Glover Reed. Trauma-informed or trauma-denied: Principles and implementation of trauma-informed services for women. *Journal of community psychology*, 33(4):461–477, 2005.

[20] Pardis Emami-Naeini, Yuvraj Agarwal, Lorrie Faith Cranor, and Hanan Hibshi. Ask the experts: What should be on an iot privacy and security label? In *2020 IEEE Symposium on Security and Privacy (SP)*.

[21] George S Everly Jr and Robert Rosenfeld. *The nature and treatment of the stress response: A practical guide for clinicians*. Springer Science & Business Media, 2012.

[22] Justin Faden and Gregg Gorton. The doorknob phenomenon in clinical practice. *American Family Physician*, 98(1):52–53, 2018.

[23] Barry A Farber, Kathryn C Berano, and Joseph A Capobianco. Clients' perceptions of the process and consequences of self-disclosure in psychotherapy. *Journal of Counseling Psychology*, 51(3):340, 2004.

[24] Jennifer Fereday and Eimear Muir-Cochrane. Demonstrating rigor using thematic analysis: A hybrid approach of inductive and deductive coding and theme development. *International journal of qualitative methods*, 5(1):80–92, 2006.

[25] Center for Substance Abuse Treatment (US). Trauma-informed care in behavioral health services, 2014. https://www.ncbi.nlm.nih.gov/books/NBK207201/.

[26] Diana Freed, Sam Havron, Emily Tseng, Andrea Gallardo, Rahul Chatterjee, Thomas Ristenpart, and Nicola Dell. "Is my phone hacked?": Analyzing Clinical Computer Security Interventions with Survivors of Intimate Partner Violence. *Proceedings of the ACM on Human-Computer Interaction*, (CSCW3), 2019.

[27] Diana Freed, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. "A Stalker's Paradise": How Intimate Partner Abusers Exploit Technology. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, CHI '18.

[28] Diana Freed, Jackeline Palmer, Diana Elizabeth Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. Digital Technologies and Intimate Partner Violence: A Qualitative Analysis with Multiple Stakeholders. *Proceedings of the ACM on Human- Computer Interaction*, (CSCW), 2017.

[29] Christine Geeng, Mike Harris, Elissa Redmiles, and Franziska Roesner. "Like Lesbians Walking the Perimeter": Experiences of US LGBTQ+ Folks With Online Security, Safety, and Privacy Advice. In *31st USENIX Security Symposium*, 2022.

[30] Sam Havron, Diana Freed, Rahul Chatterjee, Damon McCoy, Nicola Dell, and Thomas Ristenpart. Clinical computer security for victims of intimate partner violence. In *28th USENIX Security Symposium*, 2019.

[31] Colin James. Towards trauma-informed legal practice: A review. *Psychiatry, Psychology and Law*, 27(2):275–299, 2020.

[32] Shanti Kulkarni. Intersectional trauma-informed intimate partner violence (ipv) services: Narrowing the gap between ipv service delivery and survivor needs. *Journal of family violence*, 34(1):55–64, 2019.

[33] Annie Lewis-O'Connor and Elaine J Alpert. Caring for survivors using a trauma-informed care framework. *Human trafficking is a public health issue: A paradigm expansion in the United States*, pages 309–323, 2017.

[34] Bill Marczak, John Scott-Railton, Sarah McKune, Bahr Abdul Razzak, and Ron Deibert. Hide and seek: Tracking NSO group's Pegasus spyware to operations in 45 countries. Technical report, 2018.

[35] Tara Matthews, Kathleen O'Leary, Anna Turner, Manya Sleeper, Jill Palzkill Woelfer, Martin Shelton, Cori Manthorne, Elizabeth F. Churchill, and Sunny Consolvo. Stories from Survivors: Privacy Security Practices when Coping with Intimate Partner Abuse. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, CHI '17.

[36] Jill Messing, Meredith Bagwell-Gray, Megan Lindsay Brown, Andrea Kappas, and Alesha Durfee. Intersections of stalking and technology-based abuse: Emerging

definitions, conceptualization, and measurement. *Journal of family violence*, 35(7):693–704, 2020.

[37] Savanthi Murthy, Karthik S. Bhat, Sauvik Das, and Neha Kumar. Individually Vulnerable, Collectively Safe: The Security and Privacy Practices of Households with Older Adults. *Proceedings of the ACM on Human-Computer Interaction*, 5(CSCW1), 2021.

[38] Christopher Parsons, Adam Molnar, Jakub Dalek, Jeffrey Knockel, Miles Kenyon, Bennett Haselton, Cynthia Khoo, and Ronald Deibert. The predator in your pocket: A multidisciplinary assessment of the stalkerware application industry. Technical report, 2019.

[39] Safety Net Project. Tech abuse in the pandemic & beyond, 2021.

[40] Sheela Raja, Memoona Hasnain, Michelle Hoersch, Stephanie Gove-Yin, and Chelsea Rajagopalan. Trauma informed care in medicine. *Family & community health*, 38(3):216–226, 2015.

[41] Helen J Richards, Valerie Benson, Nick Donnelly, and Julie A Hadwin. Exploring the function of selective attention and hypervigilance for threat in anxiety. *Clinical psychology review*, 34(1):1–13, 2014.

[42] Mahmood Sharif, Kevin A Roundy, Matteo Dell'Amico, Christopher Gates, Daniel Kats, Lujo Bauer, and Nicolas Christin. A field study of computer-security perceptions using anti-virus customer-support chats. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, CHI '19.

[43] Daniel J Siegel and Marion F Solomon. *Healing trauma*. WW Norton & Company, 2003.

[44] Lucy Simko, Ada Lerner, Samia Ibtasam, Franziska Roesner, and Tadayoshi Kohno. Computer Security and Privacy for Refugees in the United States. In *2018 IEEE Symposium on Security and Privacy (SP)*.

[45] Julia Slupska and Angelika Strohmayer. Networks of care: Tech abuse advocates' digital security practices. In *31st USENIX Security Symposium*, 2022.

[46] Sharon G Smith, Kathleen C Basile, Leah K Gilbert, Melissa T Merrick, Nimesh Patel, Margie Walling, and Anurag Jain. The national intimate partner and sexual violence survey (NISVS): 2010-2012 state report. 2017.

[47] Emily Tseng, Rosanna Bellini, Nora McDonald, Matan Danos, Rachel Greenstadt, Damon McCoy, Nicola Dell, and Thomas Ristenpart. The Tools and Tactics Used in Intimate Partner Surveillance: An Analysis of Online Infidelity Forums. In *31st USENIX Security Symposium*, 2020.

[48] Emily Tseng, Diana Freed, Kristen Engel, Thomas Ristenpart, and Nicola Dell. A Digital Safety Dilemma: Analysis of Computer-Mediated Computer Security Interventions for Intimate Partner Violence During COVID-19. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, CHI '21.

[49] Emily Tseng, Mehrnaz Sabet, Rosanna Bellini, Harkiran Kaur Sodhi, Thomas Ristenpart, and Nicola Dell. Care Infrastructures for Digital Security in Intimate Partner Violence. In *CHI Conference on Human Factors in Computing Systems*, CHI '22.

[50] Noel Warford, Tara Matthews, Kaitlyn Yang, Omer Akgul, Sunny Consolvo, Patrick Gage Kelley, Nathan Malkin, Michelle L. Mazurek, Manya Sleeper, and Kurt Thomas. SoK: A framework for unifying at-risk user research. In *2022 IEEE Symposium on Security and Privacy (SP)*.

[51] John P Wilson, Matthew J Friedman, and Jacob D Lindy. *Treating psychological trauma and PTSD*. Guilford Press, 2004.

[52] Delanie Woodlock, Michael Salter, Molly Dragiewicz, and Bridget Harris. "living in the darkness": Technology-facilitated coercive control, disenfranchised grief, and institutional betrayal. *Violence against women*, 29(5):987–1004, 2023.

[53] Yixin Zou, Allison McDonald, Julia Narakornpichit, Nicola Dell, Thomas Ristenpart, Kevin Roundy, Florian Schaub, and Acar Tamersoy. The role of computer security customer support in helping survivors of intimate partner violence. In *30th USENIX Security Symposium*, 2021.

A Consultant Interview Guide

1. **Warm Up:** How long have you been a consultant? How does the volunteer role relate to your professional experience?

2. **Behavioral Responses**

    - Without identifying any clients, can you think of some instances where a client hass behaviors, communication styles, or emotional reactions that make it challenging to deliver technology services?
    - Are there times where you felt like attending to the client's emotional state or behaviors took precedence over providing technology services?
    - Are there times when you felt like this wasn't the appropriate service for what the client needed?
    - How do you navigate situations where there is a gap between what they believe is happening and what you see as a technologist?
    - How do you gauge clients' moods in sessions? What has clued you in to a change in mood of the appointment?
    - Are there certain indicators that you are attuned that you associate with these types of sensitivities? This can be in the referral form or during the appointment.

3. **Probing for preparation:** Consultants receive 5 hours of training on trauma interventions, as well as taking time shadowing.
    - How well did that training align with what you experienced as a consultant?
    - Are there any situations during a client session that you felt very prepared to handle?
    - Are there any situations or incidents during a client session that you felt unsure of what to do or unprepared, or like you might have not handled as well as you wanted? E.g. a client discloses ideation of self-harm (or if this has happened, what did you do?)
4. **Probing for resources:**
    - What resources do you turn to help manage these situations, either with processing what happened or seeking concrete advice?
    - Are there resources (additional training) you wish you had, but don't currently? What do you need to support your role in sessions/appointments?
    - What are some things you would like to do or say with clients but find difficult in the moment? Ex: interrupting
    - What are your go-to approaches or phrases? Were there times where they didn't work or where you felt were insufficient?
5. **Closing Questions**
    - What do you think contributes to a holistically beneficial clinic experience?
    - What would you want in an ideal world?
    - Is there anything else you'd like to tell us on this topic?

B Codebooks

The codebook for the consultant interviews appears in Figure 5. The codebook for the transcript analysis appears in Figure 6.

Theme/Code
Common client behavioral responses
Common keywords and cues
Distinguishing hypervigilance from paranoia
Anger, frustration, resentment
Intense distress or overwhelm
Anxiety, panic, or fear
Unspecified, extreme emotional dysregulation
Consultant strategies
Felt prepared and/or effective
Set boundaries with client
Try to set expectations with client
Reframe, refocus, or clarify
Provide safety information/tools
Validate client/empathy
Training and Resources
Lecture/DV 101
Field training/shadowing
Taking cases
Professional background (external)
Clinic-specific documents/resources
Clinic Structure and Ongoing Support
Buddy system
Advocate/support worker
Post appointment debrief
Clinic management
Desirables/Outcomes/Needs
Additional training
Consultant felt overwhelmed
Felt unprepared and/or ineffective

Figure 5: Codes used to analyze consultant experiences. Bolded items are high-level themes.

Theme/Code
Traumatic Stress Reaction
Hypervigilance
Exhaustion, fatigue, and resignation
Anxiety, panic, or fear
Impaired functioning/interference with daily life
Delusions, hallucinations, or psychosis
Institutional or social betrayal
Physical Symptoms
Cognitive processing issues (focus, memory)
Anger, frustration, resentment
Intense distress or overwhelm
Information dump
Self-editing
Shame, guilt, self-blame
Consultant behaviors or strategies
Consultant trying to set pace
Consultant seems overwhelmed
Consultant attempts to reframe, refocus, and/or clarify
Consultant offers validation
Consultant provides safety education, information, or tools
Consultant offering hope
Consultant setting expectations
Consultant building trust, rapport, consent culture

Figure 6: Codes used to analyze transcripts of clinic sessions.