USENIX

THE ADVANCED COMPUTING SYSTEMS ASSOCIATION

Selling the Dream: How Intimate Insiders and Identity-Based Attackers Disrupt Micro-businesses

Nazanin Sabri, *University of California San Diego;* Arkaprabha Bhattacharya and Sterling Williams-Ceci, *Cornell University;* Daniel V. Bailey, *Independent Researcher;* Rosanna Bellini, *New York University*

https://www.usenix.org/conference/usenixsecurity26/presentation/sabri

This paper is included in the Proceedings of the 35th USENIX Security Symposium.

August 12–14, 2026 • Baltimore, MD, USA

ISBN 978-1-939133-58-8

Open access to the Proceedings of the 35th USENIX Security Symposium is sponsored by

جامعة الملك عبدالله للعلوم والتقنية

King Abdullah University of Science and Technology

Selling the Dream: How Intimate Insiders and Identity-Based Attackers Disrupt Micro-businesses

Nazanin Sabri
University of California San Diego

Arkaprabha Bhattacharya
Cornell University

Sterling Williams-Ceci
Cornell University

Daniel V. Bailey
Independent Researcher

Rosanna Bellini
New York University

Abstract

Micro-businesses represent the majority of all businesses, and act as vehicles to economic freedom for many at-risk population groups. At the risk of falling behind, many micro-business owners (MBOs) increasingly adopt platforms as their primary infrastructure, and rely heavily on recruiting friends, families, and even romantic partners for running essential operations. Despite these facts, most prior work has focused on larger corporations and enterprise cybersecurity hygiene, ignoring the cybersecurity risks that such social relationships and changes in visibility introduce.

In this work, we conduct a deep dive into the experiences of MBOs through two complementary analyses: an evaluation of case records of 38 at-risk MBOs subject to insider threats, and semi-structured interviews with 16 MBOs. Our analysis show a combination of restricted access to financial resources and disruption to relationships drove them to take greater risks in recruiting and access control, leaving them more vulnerable to malicious insider attacks. They also shared that their pursuit of market reach frequently led to an unwanted, hypervisible presence, inadvertently providing intimate insiders among other adversaries with further leverage or information needed to cause harm. We conclude by proposing avenues for eCommerce governance that address these risks, focusing on preventing insider harm within these highly visible environments.

1 Introduction

Micro-businesses (MBs), defined as organizations with ten or fewer employees, constitute the overwhelming majority of economic entities around the world [15]. More than just business ventures, MBs provide an important path to independence, survival, and recovery for marginalized groups, such as women, BIPOC, and LGBTQIA+ communities [71], who face systemic discrimination. Achieving such financial independence can enable such groups to secure economically stable lives for themselves, their dependents, and their broader communities [8]. Such marginalized identities often overlap with at-risk populations — individuals who are more vulnerable to digital attacks or disproportionately harmed when they occur [10], a group that includes activists, journalists, and targets of intimate partner violence [69]. Consequently, we argue that at-risk MBs face a heightened threat landscape, making them prime targets for digital attacks.

Unlike the growing number of security recommendations for corporations [14], governments [37], or individuals [66], MBs are surprisingly absent from digital security guidance and support. This gap is especially concerning given that most MBs now launch via digital storefronts [32], and rely heavily on social media and eCommerce platforms for sales and marketing [64]. To support minority groups within these ecosystems, platforms have introduced high-visibility initiatives such as "-owned business" tags, LGBTQIA+ spotlights, and prioritized product rankings [3, 11, 60]. Yet navigating these online environments introduces a new set of security challenges [59]; work on at-risk populations including community technology [32], gig [28, 30], and sex workers [47, 48] have highlighted that increased online visibility serve as a vector for coordinated attacks. Thus, it remains unclear how adapting to these digital spaces shifts an MB's overall security posture, especially amid concerns that adversaries can weaponize the very identity markers these platforms claim to protect [47, 48]. When an at-risk entrepreneur is targeted, the stakes are notably high: the resulting loss of income can threaten the entire support network relying on them, from employees and families to local communities [48].

Thus, to ensure MBs are studied in their own right, we draw on emerging literature about enterprise security [20, 76] and at-risk groups [8, 47, 71] to ask:

RQ1: *How might visibility-driven eCommerce platforms exacerbate existing vulnerabilities and harms for at-risk MBOs?*

RQ2: *How might identity and social relationships play a role in augmenting the security posture of at-risk MBs?*

RQ3: *What solutions might eCommerce platforms offer to MBOs to alleviate harms from malicious insiders and exposure?*

To answer **RQ1**, we analyzed 38 cases from a technology clinic whom provide support for survivors of interpersonal tech-facilitated abuse (§4). To further investigate relational harms and answer **RQ2**, we conducted semi-structured interviews with 16 MBOs across a wider set of at-risk identities, honing in on the online harms they accredit to their relationships and identity (§6). Finally, we answer **RQ3** by synthesizing both data sources to present implications for platform design (§7.2) and risk mitigation strategies (§7.1).

Our findings reveal that visibility can be a double-edged sword for at-risk MBs: while vital for growth, exposure intensifies security risks through two primary drivers of digital harm. First, malicious intimate insiders (e.g., family, friends, or ex-partners [18]) use the blurring of personal-professional relationships to gain privileged technical access to destabilize MB infrastructure, often for complex social goals like control or perceived retribution for wrongdoing. Second, coordinated hate campaigns launch denial-of-service (DoS) attacks, while bad-faith buyers weaponize platform mechanisms—such as fake reviews, chargebacks, and harassment—to cause basic operations within an MB to become unstable. Ultimately, our data problematizes the prevalent eCommerce narrative that exposure equals growth and financial prosperity; instead, we find that increased visibility can scale vulnerability rapidly, exposing MBs to insider threats and targeted mobs.

Our Contribution. While prior work has helped to codify specific risk factors that constitute at-risk groups [10, 25, 71], and some of the unique vulnerabilities that small businesses report experiencing in their security posture [54, 76], no work to our knowledge has scrutinized the intersection of these two areas from a security standpoint. Moreover, prior work has mainly focused on *small* businesses which blend brick-and-mortar stores with online storefronts [54, 76], but none on MBs, especially those with at-risk identities, which have even fewer employees and resources, potentially putting their owners at greater risk of suffering harmful impacts from attacks. By listening to MBOs from marginalized groups, our data reveals vulnerabilities stemming from the intersection of owners' identities and limited resources to invest in security.

2 Background and Related Literature

A reported 99.9% of businesses in the United States are categorized as micro-businesses, employing nearly half of the American workforce [20]. In this work, we define *MBs* as independently-operated ventures with fewer than ten employees, that operate with an informal, ad-hoc management structure, and possess limited financial and technological resources [41]. While often (incorrectly) used as an interchangeable term, *small businesses* are ventures that can operate with up to fifty employees, have formal management procedures, and have more financial and technological resources [2]. Since *micro* and *small* are relative terms, definitions capture features of MBs that set them apart from larger firms [2, 17], including employee count [58], management hierarchy [41], revenue, outlet count, and public trading status [2].

The Threat Landscape for Micro-Businesses. Digital harms against marginalized businesses show up as a range of attacks that misuse platform infrastructure, social identity, and relationships to harm business health. Systemically, marginalized businesses often face administrative denial of service attacks. Adversaries may exploit platform reporting and flagging features to trigger automated suspensions [11, 57]. These attacks effectively "de-platform" businesses without a single line of malicious code, and can leverage biased moderation [6, 50] to silence creators. Such disruptions often intersect with identity-based attacks, where algorithms can be manipulated to suppress marginalized voices [24, 72] and accidentally reveal private data like mutual friends or network connections. When combined with toxic communication, increased identity-based exposure from platform interventions [11], and identity-based harassment from online trolls [42], these tactics can inflict psychological and economic damage to business owners that can outlast the immediate security incident.

The threat landscape for MBs is also complicated by the compromise of systems by trusted others [27], which moves the danger from external malicious actors to known, often trusted, internal associates. Insider exploitation involves the misuse of access by employees or known collaborators, ranging from negligent security habits to calculated financial sabotage and blackmail [8]. Levy and Schneier [39] refer to these as *intimate threats*; a new class of security threats that are exclusive to families, romantic partnerships, close friendships, and caregiving relationships. This category of threat is particularly acute in contexts of intimate partner violence (IPV). While interpersonal abuse is a broader concept that encompasses familial violence, our work focuses on the narrower scope of intimate partner violence (IPV), where former partners leverage their insider status to cause harm, such as forging invoices or filing malicious reports using the owner's own credentials [9]. These internal breaches of trust can take on the characteristics of external tactics like phishing and identity impersonation [76], which broadly aim to defraud a business by imitating its brand or leadership. Ultimately, because reputation can be a valuable currency for marginalized businesses [17], the combination of deepfakes [33], review bombing [55], and the weaponization of personal trust creates an unstable environment that threatens both the social well-being and the integrity of a business.

Challenges and Resilience for At-Risk Business Owners. Security practices in small and medium businesses are a common research focus to shape the development of more effective and suitable defenses for a wide range of business

types [19, 29, 74]. For instance, early research involving Chief Information Security Officers at small firms were the first to highlight a landscape defined by limited resources and a primarily reactive security posture [74]. This remains the case now as while many businesses use standard technical measures such as firewalls and anti-virus software, they still report struggling with regulatory requirements and the financial implications of modern security threats [29, 74]. Despite an increasing awareness of technical threats, many business owners struggle to understand the specific risks relevant to their unique scale, often underestimating their risk of being targeted by a range of different adversaries [29].

The security landscape for MBs is further complicated by the interpersonal nature of their day to day operations. In contrast to larger firms with dedicated security teams [41, 58], MBOs often navigate confusing digital ecologies solo, using consumer-grade authentication and eCommerce platforms to manage their livelihoods, as opposed to enterprise-specific services. Such a reliance on consumer-facing infrastructure often mirrors consumer habits regarding device and account sharing [46]. For instance, studies show that nearly one-third of users have attempted to access a trusted other's devices, and many individuals, including MBOs, feel that accepting these vulnerabilities is a social necessity to maintain professional and personal relationships as an expression of trust [5, 44, 45].

At-risk users are especially likely to seek economic empowerment through MBs by engaging in situated practices of resilience and agency to protect their economic livelihoods. Examples include collective organizing by BIPOC content creators to bypass algorithmic limitations [72] and "algorithmic resistance" by gig workers who intentionally ignore nonsensical platform recommendations to reassert control over their labor [28, 49]. For MBOs, security is a continuous effort to negotiate agency and safety within such platforms that often neglect their specific operational needs [25].

3 Methodology

For this work, we conducted a multi-phase, IRB-approved study to identify and contextualize the types and trajectories of digital attacks reported by at-risk individuals operating MBs in the United States. This section provides a high level overview of our approach, while subsequent sections contain further methodological detail.

Study Structure. ***Part I*** (§4) focuses on an in-depth study of MBs, examining the digital risks faced by owners who are survivors of IPV. This population group often turns to micro-entrepreneurship as an important pathway toward financial autonomy [8, 16, 22]. Using 38 transcripts from consultations with survivors of technology-mediated abuse from the Clinic to End Tech Abuse (CETA)[1], we find that MBs are highly vulnerable to targeted sabotage. We show that motivated adversaries weaponize standard platform features, such as two-factor authentication and customer review systems to exert control over a business' visibility and stability, even well after a relationship ends.

Building on the specific patterns of weaponization identified in *Part I*, ***Part II*** (§5) investigates the broader systemic failures of eCommerce and marketing platforms that enable these vulnerabilities to persist. We expanded our study to include 16 MBOs from diverse minoritized groups (LGBTQIA+, BIPOC, Disabled, Minoritized Gender) to determine if the harms faced by survivors are symptomatic of deeper platform-wide issues. Such interview participants were recruited independently from the CETA consultations investigated in *Part I*. Our interviews reveal a patchwork of eCommerce infrastructure where essential business tools–such as dispute resolution and account recovery–were reportedly unreliable, creating novel attack vectors. We also find that platform design can inadvertently promote hypervisibility while opaque metrics leave MBOs exposed to disruptions and hinder their ability to defend themselves against attacks.

Study Ordering. We chose to order our investigation in this manner because conducting a case review often serves as a crucial sensitizing phase in qualitative research [13]. Doing so enabled us to build a foundational understanding of the lived experiences and systematic barriers impacting at-risk groups, all before initially intruding into their personal lives, which can be both taxing and harmful [10].

Our analysis of case files successfully identified a common language (e.g., platforms adopted, employee descriptions) that at-risk MBOs used through written records first, which then informed how we designed our semi-structured interview guides to be more empathetic and less likely to cause re-traumatization with the groups we spoke to. Reading about written accounts prior to engagement also helps with contextual triangulation [10]: establishing a baseline of factual data from files enabled us to use subsequent interviews with more population groups to explore the why behind the trends already identified, rather than spending limited interview time on basic fact-finding. Interested readers can find further information in our Ethics Statement (Appendix 8).

Study Limitations. In *Part I*, we relied on keyword matches to identify survivors of IPV who are also MBOs. Our reliance on keywords alone may have resulted in missed or obscured cases, especially for cases who did not disclose their occupation. In addition, we chose to recruit through a tech clinic (CETA) as opposed to a support organization for MBs; although this increased the likelihood of identifying MBOs who experienced attacks, it also influenced the cases we analyzed.

In *Part II*, we recruited businesses that were operating out of a New York City, NY in the North East of the United States. MBOs were also recruited in English-language only as this matched the dialect of our research team. These factors are far from representative of all MBs; while our discoveries are

[1] https://ceta.tech.cornell.edu/

platform-mediated, the impact of location-specific concerns (e.g., customer bases), could influence our data. In addition, to scope our study appropriately, we did not speak to representatives from the eCommerce or marketing websites. Nevertheless, we would be interested to gather their perspectives to ascertain if such risks to minority businesses are already known and work towards supporting protections in this space.

Finally, for *Parts I* and *II*, our results relied on self-reporting of experiences of harms which might be impacted by participants' recollection or the degree of importance they have assigned to specific encounters. We are planning future work to employ observational studies of business operations to explore harms and real-time responses.

4 Part I: Case File Review with Survivors

Many at-risk groups face unique and socially complex attacks [71], often relying on smaller financial instruments to sustain their financial well-being. Survivors of interpersonal abuse, whom by their very nature are put at risk by being in a current or former close relationship with an adversary, are often subject to unique forms of financial and economic abuse [16]. In recent works, Bellini identifies that many of these attacks extend to their business infrastructure [8], including using mobile banking and peer-to-peer payment apps to track how and where a survivor spends money.

Survivors' backgrounds often include a uniquely dangerous malicious insider or intimate insider who has close, administrative knowledge; typically a current or former partner [9, 22, 23]. This person has access to personal data and security answers, and possesses strong, complex psychological motives to get around standard digital defenses [8]. We chose to study this population to gain a comprehensive understanding of how a determined, *intimate insider* can weaponize a MBO's digital profile to introduce unique risks.

Gaining Data Access. This investigation was conducted in collaboration with the Clinic to End Tech Abuse (CETA) in New York City in NY, US. It is composed of over 40 consultants which have supported over 1000 IPV survivors since its inception. CETA leverages its extensive evidence base to improve digital-safety outcomes through academic research, advocate training, and legislative lobbying. Tech clinics assist marginalized groups with complex technology-based concerns that can often fall through the cracks of professional services [69]. Thus, we chose this as a recruitment site due to the higher likelihood of such groups reporting their concerns.

Clients are referred to the clinic by caseworkers for interpersonal abuse (e.g., legal, housing, and counseling) once technology concerns are identified in a case. Once referred, consultants conduct 60-90 minute sessions (via Zoom, in-person, or hybrid) to assess technology concerns, identify potential compromises, and provide digital safety guidance. Clients are primarily English- or Spanish-speaking in post-separation or separation processes from an abusive partner. Participation in research is optional, and services are provided regardless of research consent.

Three members of the authorship team approached clinic leadership to suggest an investigation into attacks on MBs. Both clinic leadership and the IRB reviewed the proposal and approved the secondary use of data for this study, with the express agreement that all analyses were conducted in an access-controlled, institution-hosted cloud environment used for sensitive data.

Data and Identifying Relevant Cases. We analyzed transcripts of consultations by a technology clinic for survivors of interpersonal abuse. Any data collected in consultations only includes data from clients who have explicitly consented to participate in research. Data collection is minimized to reduce adversarial re-identification risk, so we do not report survivor demographics. Client case files include consultant notes, transcripts of recorded consultations, and referral forms, all stored in a secure, access-controlled content management system.

To collect relevant transcripts, we began by filtering the data through keywords related to financial actions (*purchase, sale, steal*), site locations (*marketplace, shop, storefront*), business personnel (*customer, colleague*), and eCommerce brands (*Etsy, Amazon*). A total of 45 keywords were used for the collection of potentially relevant cases; a full list of all truncated versions can be found in our Appendix (§3).

The first and last authors performed these keyword searches, identifying 248 potentially relevant consultations pertaining to MBs. The retrieved cases were then manually reviewed for relevance. A case was considered relevant if the survivor discussed harms experienced with relation to a MB they owned or worked for, with the overwhelming majority sharing that they were the sole owner. We identified these businesses as MBs because survivors described their workplace structures, often referencing the number of employees or co-workers involved. Borderline cases and disagreements were resolved through discussion between another two members of the research team. Our final dataset consisted of cases from 45 consultations with 38 survivors who described being actively targeted by an adversary to a business they owned or played a primary role in managing. Many survivors sought more than one consultation at the clinic, meaning that the same survivor could be present across consultations.

Analysis. Having identified 38 survivors who owned or operated within MBs, the first author then performed content analysis [36] on the anonymized transcripts of these client's consultations. Through these analyses, any segments of discussion in which survivors described attacks to their business, or attacks on themselves through their business were extracted for further analyses. A total of 65 segments were extracted through this process. Samples of the extracted segments were reviewed in weekly group meetings, and feedback was used to

Category	Harm	#	Transcript Sample
Invisibility	Denial of Account Access	11	*"I lost that number. Once I switched to [phone operator], they told me that because he was the primary account holder on that account, that this belongs to him. So I lost all my business cards because I can't have that number anymore"* (C_{12}).
	Deletion of Business Data	6	*"last summer I started having people tell me that they had emailed or texted me things and I wasn't getting them and I couldn't find them in my emails"* (C_3).
	Termination of Business Operations	4	*"I even have a business page that they deactivated, because that was public"* (C_1).
Hypervisibility	Impersonation of Business	10	*"He's opened accounts in my name and my social and he took the company I had that he hacked and he did fraudulent loan security on that company"* (C_4).
	Remote Surveillance	9	*"I have a big social media presence and that's how I make money ... I want to do everything by the book ... but that's my livelihood where a chunk of my income comes in ... to get out of my situation and save my money and flee"* (C_{35}).
	Close-Range Monitoring	7	*"I ended up finding out that for a really long time, he's been going through all of my accounts just keeping tabs on me on who I was messaging. You can look up pictures that you like and things that you leave comments on"* (C_7).
	Unauthorized Financial Expenditure	3	*"She removed [the] Wi-Fi card from the laptops ... this keeps our devices connected and our store running ... that move cost me a fortune"* (C_6).
	Promoting Falsehoods Online	2	*"they [used] my business email address and posted on this blog and said my boyfriend cheated on me with an actress which is not true"* (C_{10}).
	Harassment of Employees	2	*"he sends text messages to everyone, including ... my employee, employers and my coworkers ... it was awful, I couldn't work"* (C_{33}).
	Harassment of Clients	2	*"on my business website, I had a chat feature and I had to take it down because he was using that to communicate with my clients"* (C_5).
	Threats to Physical Harm	2	*"he kept texting me saying, "If you don't talk to me, I'm going to do this""* (C_{11}).
	Non-consensual Sexual Content	2	*"I was signed up for subscriptions [...] there were sexual ones [too]"* (C_{10}).

Table 1: Business-based harms by interpersonal abusers. A total of 38 cases were analyzed for the extraction of these harms. The research team qualitatively categorized harms into (a) invisibility and (b) hypervisibility, each discussed in Section 4. Within each category harms are ordered according to frequency. Samples have been lightly reworded to preserve anonymity.

re-analyze the transcripts and ensure all relevant information was captured. The first author then clustered these segments, using inductive coding, into the type of harm being imposed, creating 12 clusters of attacks on MBs (Table 1). The last author provided feedback throughout the process, reviewing coherence, independence, and clarity of created clusters.

4.1 Part I: Case Findings

Our analysis show that active adversaries, like abusers, can exploit the policies and design of eCommerce platforms to sabotage survivors. We find that survivors report contradictory pressures on themselves and their MBs. On one hand, adversaries forcibly attempt to make their business *invisible* (§4.1.1), stripped of access to tools and platforms that sustained their business. Yet on the other, they reported feeling *hypervisible* (§4.1.2), exposed to unwanted surveillance through their professional presence online, which made them a further target for motivated adversaries. Thus, survivors were left without control of their visibility to manage their security posture; a phenomena also witnessed with racialized minorities [11]. C_i is used to differentiate specific cases.

4.1.1 Erasure through invisibility

Abusers were described to impede business activities, even causing the business to shut down fully. This interference was either done directly or by creating so much fear that the survivor reported feeling unable to continue running the business. In the case of direct interference, C_{12} described operating their business using a phone line that was on a phone plan shared with, and owned by, their abuser. Once they separated, the abuser refused to transfer the phone number to the business owner. The phone company was also unwilling to assist C_{12} as in their view *"[the abuser] was the primary account holder"* (C_{12}) and thus legally owned the number.

Another example of direct interference was described by a survivor in relation to their MB, about an abuser who *"hacked into everything of mine and put his own information on my storefront"* (C_{32}), alongside denying them access to their enterprise account. This attack left a survivor unable to *"change the password or re-gain access"* (C_{11}) despite being the original owner of the business. Subsequent loss of access to assets (e.g., internal revenue service account, business cards) was also brought up by many survivors as being *"financially devastating"* (C_3) and disruptive to their eCommerce store.

Direct manipulation and interference was not the only way in which abusers hampered business operations. Survivors also described being overwhelmed from managing their safety, and owning a business resulted in them making the decision to *"slow down on everything, because I don't know exactly how to handle all this"* (C_2). These feelings of confusion, overwhelm, or fear would at times result in changes to operations (e.g., removing chat features from their website) or complete termination of the business. As one survivor expressed in exasperation: *"... well it's a public store account, surely he will find ways to look at it and contact me"* (C_{25}).

4.1.2 Overexposed through hypervisibility

Not all survivors reported closing their business as a result of such insider harms. Some expressed feeling conflicted between their personal privacy and visibility of the business, with one owner of a bespoke gifting service sharing *"for my business there's stuff I can't make private"* (C_5) without jeopardizing reach. Even though many survivors reported feeling *"conflicted"* (C_{35}), and wanting to *"do everything by the book of domestic violence victim"* (C_{15}), ceasing business operations would mean the loss of an economic livelihood.

To manage the challenges of being visible while also being safe, survivors attempted to remove information that could be used to harm them. This was in acknowledgment of the potential shortcomings of these methods. As C_5 shared when referencing their store's physical location: *"I secure up my data as best I can [...] he knows the neighborhood I live in [...] so everything counts"*. This concern for an adversary knowing their physical location also led C_{19} to scrub public records surrounding their business operations out of fear that *"there's just a single location [the adversary] might recognize"*.

Survivors also shared that adversaries would contact the business as a customer *"to inquire about some of my products"* (C_4). Such adversaries could also recruit a member of their wider and shared friendship group to take their place around such inquires; Freed et al. [22] refer to such attacks as *abuse by proxy*. As C_4 shared upon receiving a request for an order, they *"respond[ed], thinking it was a purchasing customer"* yet felt ashamed that they could not differentiate the customer from a live attacker once the attack was revealed.

In addition to fears of surveillance on online platforms, survivors discussed specific, socially-targeted attacks they faced via platform tools. Many survivors recounted how their abuser spread rumors about their business and themselves as the owner. For C_4, a survivor who owned a brick-and-mortar business, they reflected that *"[my former partner] created an account using a similar handle to the organization"* to deter customers. In a similar vein, C_{14} also described how online rumors were targeted at their online business, whereby their abuser taunted them online *"to try and defame both my current partner and I and our business"*. Survivors were even put in challenging social circumstances with their colleagues when abusers contacted the survivors' colleagues *"to sabotage me [...and] give me a bad character"* (C_{21}).

5 Part II: Interviews with MBOs

We identified from *Part I* that survivor-owned MBs felt like they had little to no *control* over their visibility, leading to either invisibility (§4.1.1) or hypervisibility (§4.1.2) which impacts their security posture. We also identified that they are at a far greater risk of unauthorized account access than even prior literature has suggested [8]. Our findings identified that the attacker was either: trusted with the credentials at some point during the relationship, or knew the MBO enough to be able to guess knowledge-based authentication secrets (passwords or security questions) and gain access. While we confirm the presence of such attacks in prior work [22, 23], our findings highlight how eCommerce platforms leave at-risk MBOs vulnerable to account takeover, impersonation, and loss of income while they work to re-gain access to their accounts and trust from buyers.

Thus, we tailored the design of *Part II* into investigating eCommerce risks more broadly, but dedicated time to investigating two pressing areas: insider harms and visibility-based attacks. Here we report on the findings of our semi-structured interviews with 16 MBOs around the specific challenges with use of eCommerce platforms. Semi-structured interviews allowed participants to narrate their experiences at their own pace and provided the opportunity to dive into the structural pressures that can force owners into adopting riskier postures.

MB Identification & Recruitment. Our participant pool was scoped to business owners who face a higher risk of harm from technology (as highlighted by Thomas et al [66]). We used several business directories from organizations in New York, NY in the US to identify businesses meeting this inclusion criteria. These included dedicated directories for minoritized ethnic groups, certification programs for minority- and women-owned businesses, and directories for businesses registered with local chambers of commerce. To catch organizations that may not be listed, we turned to ChatGPT, which has demonstrated efficacy for search tasks [75]. We constructed four prompts to query ChatGPT between March – October 2025, and selected the *gpt-4o-latest* model for queries.

Three members of the research team carried out the business selection process. On each business directory, researchers scanned the output for relevant businesses, visiting any publicly-linked websites or social media profiles of the business. For each recommendation from ChatGPT, the researcher would first cross-check the business with Google to limit the impact of model hallucinations [31], and visit any linked websites or social media profiles. Researchers remained lenient in this first pass, only excluding businesses that had more than three locations, or explicitly described more than ten active employees (alumni were considered as former employees). To identify if the owner was at-risk, the researchers read owner profiles on the business' online webpages, noting whether they publicly identified as being at-risk (e.g., BIPOC, LGBTQIA+, a woman, or a survivor of IPV). In total, we found 103 businesses, 32 of which came from ChatGPT and 71 from the business directories we scanned. Eighteen of the businesses found by ChatGPT were also co-located in one or more of these directories.

We drafted interview request emails for each selected business, including an overview of the study, why the business was selected, a link to a pre-interview screening survey, contacts of the research team, and a link to schedule interviews. We also used snowball sampling and flyers at small business

ID	G	Race	Business	Em	Y	Sales	Marketing	Threat Vector ($\mathcal{T}$)	Mitigation ($\mathcal{S}$)
P1	F	AAPI	Handmade Jewelry	5	1	E	IG, TT	Harassment	Content Filtering
P2	M	White	Custom Keyboards	6	1	E, SH	RD, TT	Harassment	IP Blacklisting
P3	F	Af. Am.	Sleep Products	1	2	SH	IG, LI, FB	DoS, Insider Threat	Legal Remediation
P4	F	Lat	Baby Clothes	9	–	SH	IG, FB, TW	Harassment	Discontinue Sales
P5	M	White	Designer	9	1	SH	IG, TT, FB	DoS, Harassment	Platform Diversification
P6	F	AAPI	Custom Stationery	8	1	E, AM	PI	Fraud	Platform Migration
P7	NB	Af. Am.	Queer Apparel	4	2	E, SH	IG	DoS, Harassment, Fraud	Platform Migration
P8	M	AAPI	Coffee Roastery	9	3	WIX	PI	Insider Threat, Lockout	Recovery Protocols
P9	F	White	Private Therapy	3	7	–	–	Fiscal Insider Threat	Access Revocation
P10	M	White	Construction	6	6	WIX	LI	Harassment & Spam	Physical Security
P11	M	Lat	Tiling Business	7	8	–	IG	Fiscal Insider Threat	Platform Migration
P12	F	Lat	Online Retail	5	2	E, SH	RD, PI	Insider Threat	Access Revocation
P13$^{\delta}$	F	White	Pottery	2	2	SH	IG, PI	DoS, Insider Threat	Access Revocation
P14$^{\delta}$	F	AAPI	Pottery	2	6	SH	IG, PI	DoS, Insider Threat	Access Revocation
P15	M	-	Designer	5	2	SH, EB	IG, LI	DoS, Harassment	Operational Scale-down
P16	F	AAPI	Brand Consultancy	3	6	Ecwid	IG, LI	DoS, Insider Threat	Access Revocation

Table 2: Interview participant information. $^{\delta}$ indicates participants interviewed together; – indicates participant chose not to disclose details. Employee count (**Em**) includes the owner. Gender (**G**) and Years of Experience (**Y**) were both asked directly of participants. $^{\delta}$ indicates joint interview; – indicates participant chose not to disclose details when asked. The Sales and Marketing columns list the platforms MBOs used for those purposes, respectively. Shopify and Etsy were the most used sales platforms, and Instagram was the top marketing platform among our interview participants.

support centers, recruiting a total of 16 participants (Table 2).

The majority of our interview participants (N = 11) were recruited through the aforementioned strategy. However, five participants were referred by other interviewees (snowball sampling) who, once they understood the focus of our study, referred acquaintances they were aware had experienced harms related to their businesses.

Data Collection & Analysis. Three members of the research team carried out 15 semi-structured interviews with 16 MBOs over Zoom (N=12) or in person with online audio recording (N=4) between June 2025 and January 2026. Two participants (P_{13}, P_{14}), both MBOs of separate ventures chose to be interviewed together to provide each other emotional support. Each interview lasted between 41 and 76 minutes (M:61; SD:4.5). All participants were over the age of 18, resided in the US, and spoke English. Participants also covered a range of minoritized gender, sexualities, and racialized identities.

Interviews began with questions surrounding the origins of their business, their adoption of technology for business and marketing, and, if appropriate, their process of on-boarding a trusted individual. We probed participants using the Critical Incident Technique [21] in which participants were encouraged to reconstruct a challenging security incident involving technology abuse (either by a trusted individual, or by an external threat) to minimize recall bias and capture relevant data. We also listened to potential steps for resolution to such an attack, such as protective strategies or reporting such incidents to the eCommerce platforms. We chose to not use loaded terms such as 'scam' or 'attack' [76] to avoid priming participants in their answers and remain sensitive to owners who may not describe their experiences as abuse. Participants received $40 in compensation.

Analysis. Three members of the research team then used reflexive thematic analysis [13] to identify broad themes within participant accounts. A sample set of codes was initially generated via coding two interviews. After discussing these codes, another three interviews were coded independently and the same discussion and disagreement resolution process was repeated. The last author then reviewed the codes and held discussions with the three annotators, providing feedback until agreement on codes and definitions was reached, resulting in a final stable codebook of 33 codes (e.g., credibility and trust, giving up on solutions, and lack of control).

Two members of the annotation team then separately annotated all fifteen interviews, meeting weekly to discuss disagreements and insights. Themes were developed through discussions between all members of the research team (§6).

6 Part II: Findings

Our interview findings reiterate the experience of survivors in *Part I* (§4), that many MBOs navigate complex personal relationships while also attempting to run a successful business online (§6.1). Participants described a diffusion of responsibility for security across personal relationships, which then

lead to increased risk-taking across hiring, account management, access revocation, and re-securing an online business. In fact, our findings highlight that as soon as the health of the relationship was jeopardized (even outside of a romantic context), there was an increased risk of financial sabotage.

Alongside managing malicious insiders, MBOs also reported a specific type of removal of control of their store visibility; identity-based targeting which lead to a malicious form of denial of service attacks (§6.2). We identified that such attacks were experienced as de-platforming; efforts to make the MBO invisible (akin to the survivor reports in *Part I*), irrespective of the adversary's personal relationship to them. We also discover that eCommerce platforms seemingly adopt design patterns focused on solo authentication and access management that could inadvertently contribute to how easy these attacks were to perform.

6.1 Intimate Insider Sabotage

All MBOs that we spoke to shared that they lacked a formal human resources department, and often relied on personal connections (friends, family, or acquaintances), simply because they were already known, instead of using professional vetting (§6.1.1). While participants shared that this choice greatly simplified the onboarding process, many admitted to give unrestricted access based on personal trust rather than actual need (§6.1.2). Because these connections are based on social ties, participants described being reluctant to impose access controls even during attacks (§6.1.3), with some sharing that imposing them felt like an act of distrust or a betrayal of personal relationships.

6.1.1 Hiring of Convenience

We found that participants regularly chose the path of least resistance over formal competency checks for recruitment, describing their practices as *"a mess of convenience over security"* (P_{16}). Participants admitted during the interviews that they prioritized social and geographic proximity as a reliable sign of professional integrity. As in many cases, participants described that hiring decisions came from emotional or logistical responses to burnout rather than being strategic business moves. Since the candidates were already part of the owners' social or romantic circles, the usual challenges of recruitment, like background checks, references, or technical assessments, felt unnecessary or even inappropriate. As P_9 mentioned, because their partner had the right background and noticed they were *"drowning in billing and insurance claims,"* the hire *"felt like a no-brainer at the time."* Similarly, P_8 admitted that knowing the person they hired created a psychological blind spot, saying, *"the person in question was a friend of a friend ... Maybe that's why I let my guard down."*

This reliance on social proof led some participants to a halo effect [51]; where a hire's likability was often confused or even conflated with professional reliability. Participants noted that the immediate relief these hires provided, like handling social media or administrative tasks, hid the risks of mixing their personal and professional lives. For example, P_4 mentioned that a recent hire, who was an acquaintance, was initially *"friendly with customers and even helped boost our Instagram following,"* which further supported the convenience of the choice. P_9, when discussing hiring their partner, added that the hire's presence in their home made the transition to the workplace feel easy: *"It came up at home anyway, how stressed I was [...] He was a real go-getter and did everything for everyone [...] It made sense at the time"*

This avoidance of boundaries was often described as a collaborative dream, but it put the business owner at risk of exploitation when the relationship changed. P_{12}, who co-owned a business with their partner, noted that this framing is *"already part of the problem,"* as it rationalizes the abandonment of clear roles and boundaries. P_{15}, whose partner joined the business six months after launch to support their technical needs, summed up this vulnerability as a *"trust paradox,"* explaining that *"the whole 'own business' dream is built on collaboration."* As P_9, who had hired their then-romantic partner, lamented:

> *"It was me giving someone access because of who they were to me, not because of a formal vetting process [....] I realize now how stupid that was"* (P_9).

6.1.2 Privileged Account Management

Even well-funded enterprises struggle with privileged account management [43]. Our results show the problem is exacerbated in MBs, in part due to lacking dedicated IT staff. Our participants described feeling overwhelmed by the extensive list of tasks business owners need to engage in. All these demands led them to grant unrestricted access to the technical infrastructure of their business, which resulted in abuse of system-access privileges.

In support of other adjacent privileges [27], we found that MBOs described giving broad administrative permissions based on personal relationship instead of job-role necessity, which included employees being granted admin access to sensitive systems such as the business's website, or financial accounts which were then exploited. In some cases, access was set up for a partner, who later leveraged it after the relationship broke down. As P_{15} described the initial set up:

> *"We met [..] six months after I launched. He [was] very tech-savvy [...] and at the beginning, it was just perfect. He'd come over after work and I'd be struggling with some CSS glitch on a client's landing page or trying to figure out why my email automation wasn't firing, and he'd just fix it"* (P_{15}).

Many of our participants disclosed the psychological and social tension linked to enforcing formal security protocols, a finding consistent with earlier results. Prior work has identified trust as a performative act in human relationships that extends to consumers sharing devices, accounts, passwords, and PINs [44]. This tendency extends to intimate partners, where showing vulnerability and visibly taking on risks are seen as essential parts of relationship-building [53]. So much so that some participants shared that mitigating such risks felt like an insult to the relationship. P_{15}, described choosing to focus on the product and delegate technology tasks to their partner, explained:

> *"You don't think 'I should really silo my administrative privileges just in case this person decides to weaponize my livelihood"'* (P_{15}).

The shift from shared trust to professional crisis often stemmed from platform designs that depend on consumer-level authentication. MBOs described using platforms that use a single username-password combination, creating an 'all-or-nothing' delegation model. P_{11}, whom also left technology tasks to a contractor who then sabotaged parts of the organization, described this as *"incredibly dangerous"* because it *"bypasses every safeguard [...] like least privilege and compartmentalization."* Such a design can push owners to choose between cutting off a new enrollee or risky transparency that could be later weaponized. P_{12} explained that in a joint venture:

> *"you're not granting access; you're sharing authorship. And authorship comes with entitlement... to systems [and] control"* (P_{12}).

P_{12} reflected that this discomfort frequently led to a *"convenience-first"* approach, where *"every security action [felt like it] had a symbolic meaning,"* and revoking credentials for their partner and co-owner felt less like a professional requirement and more like *"cutting [them] out of our shared history."* Similarly, P_9 pointed out that the personal nature of their bond made formal oversight feel awkward. This led P_9 to address technical slips in *"one-on-one chats, not formally,"* which allowed the insider to carry on fraudulent activity under the pretense of *"benign errors"* and typos.

6.1.3 Picking Up the Pieces of Internal Sabotage

When personal relationships fell apart, owners reported encountering substantial tensions with platform infrastructural design. P_{12}, who again focused on the creative aspects while leaving technology tasks for their partner, lamented: *"I didn't have a mental model for someone who loves you but is also going to wreck your business."*

A disconnect between infrastructure and expectations was also reported by participants in the language and reporting to the platform they used. For example, when P_9 attempted to report uncleared or maliciously refunded transactions, they found that their payment processor did not have any category for internal sabotage. Participants argued that this lack of categorization forces platforms to either see betrayal only as a personal failure on behalf of the seller instead of a failure in access control, or to see it as:

> *"account compromise, which means our account now has a security incident flag and [...] we're considered high risk."* (P_9).

As a result, participants shared feeling there were many forms of institutional victim-blaming where accounts face permanent penalties. In the same vein, P_8 noted the following in the aftermath of a malicious insider attack and the subsequent impact on their business:

> *"My account has a permanent record of a 'security incident' [...] I'm considered high risk [...] higher fees, longer payout delays, even account termination. And all because there's no mechanism for 'this was an inside job.' It's absurd!"* (P_8).

Participants who experienced insider attacks also struggled with access revocation. MBOs who use multiple platforms to run their business were especially susceptible as they lacked a complete view of the ongoing access available to the insider. Each platform relies on its own authentication methods leading to *"technical residue"* (P_{12}) like old admin accounts and API keys that become permanent parts of the *"insider-risk surface"* (P_{13}). P_{15} describes that this residue could include the creation of hidden accounts that maintain access even after a romantic or professional relationship ends. In extreme cases, failures in platform authentication could lead to complete lockouts. P_3 described a friend and fellow MBO who was *"out of business for a while"* because they could not prove their legitimacy to a web-hosting system that only recognized the attacker's credentials.

Beyond technical challenges, participants also discussed an aftermath of lasting reputational damage. When a former employee created copycat accounts on social-media sites with similar names in order to contact and scam customers, P_{11} found the platform's takedown response to be inadequate. They described it as a *"whisper after a megaphone blast"* that left the owner to handle their damaged reputation entirely by themselves. Participants described how the resolution of an insider attack often went beyond digital security, leading owners to: *"quietly talk to other small business owners... not for security, but for abuse"* (P_{12}).

6.2 Identity-Based Targeting

Many MBOs that we spoke to also disclosed another form of identity mixing; this time a conscious choice to make their identity visible, and in some cases, part of their product lines

(§6.2.1). This in turn led them to gravitate towards other communities of sellers on eCommerce platforms (§6.2.2), but also be targeted through DoS attacks based on features they reported being unaware of (§6.2.3). Participants explained that such visibility-based attacks were hard to recover from (§6.2.4), particularly when platform responses were absent or perceivably ineffective.

6.2.1 Mixing Personal and Business Identities

Most MBOs we spoke to tied their business closely to their identity and values. P_4 reflected that in their enterprise that sold baby clothes how *"the company is me like there's no division."* P_1, a seller of handmade jewelry online also reflected that their business *"isn't just a business. It's my livelihood, my art, my identity."* Owners also shared how their personal identity impacted how they operated and presented themselves online, such as sharing content on social media platforms showing *"behind-the-scenes videos or little stories about where a design comes from"* (P_{11}). However, the pressure to perform a specific form of identity weighed on many sellers where sharing identity-related content would feel forced or need to be constantly defended, as P_1 shared being *"expected to explain or justify your cultural choices more"* and being assigned the role of *"cultural ambassador."*

MBOs in our sample nevertheless shared a sense of pride and empowerment associated with having a large number of responsibilities; as P_{11} disclosed, they *"wore multiple hats."* When talking about having to manage multiple in-person and online sales channels, one participant expressed being *"exhausted, [...] but it's good tired, the kind of tired that feels earned"* (P_7). This exhaustion, however, led many participants to share their struggles to manage the wide range of operational domains at once: from product design (P_5), inventory management (P_{10}), marketing (P_1), customer service (P_6), and incident response: *"if something breaks, or a [customer] is upset about [something], it lands on my desk"* (P_9).

6.2.2 Weaponizing Customer-Protection Policies

To reach a wider customer audience, sellers would share content on platforms. P_6 stated: *"a single reel could go viral and I'd get ten or maybe twenty times my usual orders,"* and they would likewise hold back from sharing such content if *"it didn't drive meaningful traffic."* Participants also expressed preference for platforms that improved the perceived credibility of sellers: *"for Etsy at least, you couldn't move in artisan circles without someone mentioning it"* (P_1).

Increasing the reach and visibility of the MB also came with a trade off; participants who used eCommerce platforms overwhelmingly described challenges navigating how platform policies functioned, especially across different platforms. Sellers expressed feeling like customers would deliberately *"test the boundaries of what was acceptable"* (P_{12}) due to weak enforcement of platform policies that favored sellers. For instance, customers would file falsified disputes to receive a refund or cause disruption to the business process. P_6 recounts how some customers explicitly *"say things like 'I'll just open a case and Etsy will refund me anyway.' And they're usually right."* Others described filing a dispute despite having seller policies clearly communicated, and still succeed:

> *"I had a customer who modified the [key]board I sent them [...] and then tried to return it. I explained that modified items aren't returnable. They filed a dispute and won"* (P_2).

While participants were cognizant of both the business benefits of exposure and the risks, participants including P_2 noted being unaware of risks posed by customers until an attack had occurred. Our participants perceived that customers knew that platforms put more power in the hands of buyers, allowing them to *"test how much you're willing to give"* (P_6). While such policies are valuable in protecting buyers from orders that are not delivered, arrive damaged, or do not match the listing description [1], many participants cited examples that such policies often did not consider bad-faith buyers as a result of increased visibility.

> *"It's designed around buyer retention, not seller stability [...] It's like they think: 'The customer brings the money. The seller is disposable' "* (P_2).

We saw that customer-protection policies came with costs beyond just monetary, including being evaluated on criteria the seller did not initially understand. These areas of confusion left sellers concerned that they could be weaponized by online adversaries. As one reflected, they felt like they were *"walk[ing] on eggshells"* (P_{14}) to please customers, out of concern for potential backlash against their storefront. While some participants decided to leave their preferred platform due to this tradeoff, others stayed despite customer misbehavior, as shared by P_{12}: *"I've thought about [leaving Etsy] a lot. But discoverability is hard without them."*

6.2.3 MBO Denial of Service Attacks

Beyond dealing with difficult customers, our participants recounted explicit attempts to harass the MBO, disrupt business operations and a lack of effective countermeasures. The increased visibility that comes from joining an eCommerce platform induces its own risks, by creating visibility that *"turned really hostile"* (P_2). We identified a pattern of bad-faith buyers who harm an owner's reputation, causing platforms to deny service to them or other customers to attempt to pressure the organization to leave the platform. Our participants reported that some customers *"weaponized"* (P_6) platform policies to harm the reputation of their MB , and personally attack the seller. Participants disclosed they suspected the attacks were motivated by hate or disagreement with their identity.

Participants also described customers who leveraged a range of different features, particularly, *"the refund process, the reporting tools, the review system [...] All of that gets flipped"* (P_7). Some customers would even purchase items in bad faith, often with new accounts each time, just to leave harmful comments in messages-to-sellers and reviews. P_7, a seller for queer apparel across Etsy and Shopify who experienced malicious chargebacks, recalled a customer who *"tried to purchase everything in the shop [...] and then immediately initiated a chargeback just to cause disruption."* They theorized that this was intended as a tactic of coordinated sabotage, that attempted to get a business flagged as fraudulent by the platform and accompanying payment processors:

> *"People will flood your store with fake orders, max out your inventory, then initiate mass chargebacks to trigger automatic fraud flags. The goal isn't to get the stuff [...] It's to get your account suspended. To cost you money"* (P_7).

Such types of attacks were often identity-motivated based on the number of slurs described in the attack and highly coordinated by off-site groups. While refund abuse and harassment occurs across eCommerce, our participants shared how their identity afforded them an acute form of harm. P_7 reflected that these coordinated attacks were likely a deliberate threatening strategy to at-risk groups, noting, *"I think [DoS'ing] is a known tactic in far-right online organizing spaces, apparently–weaponizing eCommerce systems"*. Another participant argued that the platforms that they had chosen felt structurally inadequate to handle such campaigns that targeted their marginalized identity, noting: *"[platform hosts] treat each event as an isolated incident, so the scale and coordination gets totally missed"* (P_1). Beyond technical disruption, participants also highlighted grave threats to their digital safety, as P_5 reflected: *"when it comes to Race-based, cultural-based, and death threats"* they felt that platforms failed to notice them and take adequate action.

Participants mentioned that their reputation is an important consideration when running their business. While larger businesses may be less affected by negative engagement from customers, it was reportedly costly for MBs. P_2, who had just started a new business for custom keyboards lamented that a *"bad review can tank your traffic,"* meaning that *"abusive customers have all the leverage"* even if said customers were reportedly dissatisfied with *"unreasonable expectations around seller responses"* instead of the *"actual product."* As another participant when asked about customer relationships reflected, *"if people don't think you can deliver, they just move on"* (P_8). Thus, mitigating the impact of weaponization often meant identifying ways to preserve a seller's reputation, but with seemingly few technical options.

6.2.4 Recovering from Visibility-Based Attacks

Our participants expressed difficulty in recovering from visibility-based attacks and believed that platforms could offer better tools. P_7, a queer apparel seller who had a bad-faith customer attacking them for their identity by *"buying stickers, then leav[ing] one-star reviews that say things like 'this is demonic' or 'you're a disgrace',"* illustrated this inability to address the issue:

> *"On Etsy, you can block someone from messaging you, but you can't stop them from placing an order. So even when it's clearly targeted harassment, they can just keep buying the cheapest thing in the shop and using the review system to spread hate"* (P_7).

As many sellers closely tied their business to their personal identity and values, these attacks could lead them to abandon platforms: P_7 ultimately left Etsy for *"Shopify [which] doesn't give you buyer-blocking tools either unless you install third-party apps."* Even if these add-ons are used, blocking is *"mostly based on IP or email, which doesn't help when someone's determined"* (P_7). The participant expressed surprise that *"none of these platforms imagined that small sellers could become targets for harassment"* (P_7).

This feeling of abandonment was echoed by a number of participants, feeling like the *"platforms just seem to turn a blind eye to it"* (P_5). Participants also expressed a belief that support hinged on their reach and *power* on the platform:

> *"If you're not a creator with a million followers or a big brand with ad spend, you're invisible to them. They say they care about safety, but the reporting tools are so shallow. There's no one to talk to"* (P_1).

This made sellers feel like they were *"screaming into a void"* (P_1) (akin to [50, 70]). Even when the platform did intervene, the seller was *"stuck waiting days, sometimes weeks, while [their] livelihood hangs in limbo"* (P_7).

7 Discussion

Our study across *Part I* and *II* identifies three primary drivers of digital harm for at-risk MBs: customer-/insider-initiated exploitation (§6.1), a lack of control of visibility (§4), and the ability to recover quickly on platforms (§6.2). We found that while visibility is vital for growth, it becomes a double-edged sword which intensifies security risks for such groups, especially at the intersection of interpersonal abuse [22, 23].

While our findings highlight harms targeted at identity-forefronted businesses (e.g., women- or Black-owned), the mechanisms of abuse—such as refund fraud and disruptive disputes—could be deployed against any online merchant for non-identity-based reasons. Consequently, our findings may be used to support any MBs. Building on existing literature

regarding at-risk groups [8, 26, 47, 71], we explore how platforms can facilitate visibility while mitigating coordinated, identity-based harassmentt [26, 48]. Specifically, we propose improving platform tools to counter coordinated attacks, refining seller policies to prevent malicious exploitation, and strengthening identity and access management, particularly against intimate insiders.

7.1 Identity and Access Management

Our study highlights that MBOs face insider harms arising from a blending of personal and business relationships. To date, most literature on insider attacks focuses on those motivated predominantly by financial gain. Yet our work shows MBOs struggle with different challenges when a personal relationship deteriorates and affects the business.

7.1.1 Addressing Intimate Insiders

ECommerce platforms often assume that the primary risks to sellers come from external actors. While existing research has examined interpersonal harm in domestic (e.g., intimate partner violence and technology abuse [22, 23]) and organizational settings (e.g., insider threats in enterprise security [65]), the unique blend of business and personal challenges our participants reported remain largely unaddressed.

Identity and access management, which encompasses user authentication and authorization, is an ongoing challenge, even for enterprises with significant resources [65]. A consistent pattern in our study was that most access management harms stemmed from adversaries within the business's social or familial orbit. Thus, our findings speak to works on gig workers [30], community technology workers [28], and sex workers [47] that show how resource constraints amplify vulnerability to insider exploitation.

Building on the study of 'proximate' adversaries in prior work [9, 22, 23], we argue that platforms should incorporate mechanisms for access control, role differentiation, and rapid response that account for trust eroding over time. For instance, platforms could introduce a role-based access where sellers explicitly assign and revoke limited roles (e.g., fulfillment, messaging, advertising, inventory), and are nudged to reconfirm roles. Industry standards (ISO-27001) and regulatory regimes (HIPAA) require periodic access reviews, with the usability community offering insight into how to make nudges less stressful and more time-effective [7]. Facilitating this practice for MBs would prevent abusive partners or contractors from gaining overlooked privileged access. Sudden changes in access (e.g., account number change) could trigger an alert that asks the business owner to authorize the change, and otherwise provide instructions for remediation.

7.1.2 Immediate Authentication Changes for MBOs

As reported by our participants, the flat access model implemented by some platforms encourages sellers to share their credentials, which goes against security best practices [52, 54, 61]. Credential sharing is a well known risk within such environments, especially when an individual account is far more affordable for low-income organizations that cannot afford costly enterprise, multi-user services. Yet our participants mentioned such a flat model contributing to financial loss and expressed a desire for more flexible, hierarchical access control, such as role-based access control and limited-privilege accounts (e.g., order fulfillment without payments). Some platforms such as TikTokShop already implement this feature suggesting its feasibility for future sites [68].

Many novel authentication approaches focus on a device-as-authenticator over knowledge based attacks whereby there is a physical limitation to credential sharing. For instance, passkeys are often suggested as a replacement for passwords as they cannot be shared easily between different users. However, such alternatives should be recommended in such context with great caution. Platform support for these mechanisms is not only inconsistent (e.g., Etsy does not support passkeys but TikTokShop does [1, 67]), but passkeys themselves do not prevent intimate insiders who often can enable access to a physical device of an at-risk seller and add their own biometrics for immediate and continued access [5, 8]. To prevent this type of account hijacking, platforms could use periodic biometric verification beyond signup or account recovery time [1, 67].

When dealing with former or abusive intimate partners, our participants expressed fallback authentication such as personal-knowledge questions being a vector of compromise [38]. Researchers have long identified the shortcomings in these approaches which unfortunately persist today, meaning that novel technology design that presume frequent compromise via physical access to a single personal device, and the ability to know specific secrets such as password. Platforms should take into account the need to revoke use of fallback authentication for MBOs.

7.2 Safer Platforms for MBOs

Our participants reported exposure to DoS in the broadest sense: attackers disrupted business operations through harassment, fraudulent reviews, business impersonation, chargeback scams, and other tactics. Inspired by work on platform governance and algorithmic visibility [11, 34], we discuss design interventions that balance discoverability with safety.

7.2.1 Visibility Without Vulnerability

ECommerce platforms might elect to promote woman- or BIPOC-owned businesses on their first page or push content to make it go viral. While these mechanisms of creating visibility could be fruitful for both sellers and platforms (e.g., sale

commissions, retaining fee-paying sellers), these initiatives made some of our participants targets of DoS attacks. Woman- or BIPOC-owned tags could make sellers hypervisible to users who engage with them in bad faith, causing psychological and financial harm [3, 11, 60]. Such design choices cause recommendation algorithms to become unintentional catalysts for attacks that threaten digital-safety.

Future work on securing platform design could investigate methods for affording visibility to sellers while avoiding potential backlash from bad-faith buyers. One suggestion could be to factor buyer reputation into recommendations, similar to how user reputation is tracked on social media (e.g., Reddit's karma system [56]) and Q&A platforms (e.g., StackOverflow reputation [62]). Personalized and character-based recommendations have been implemented in other professional contexts such as job searches. Platforms could assign lower reputation scores to bad-faith buyers and use these signals to reduce susceptibility to the class of denial of service attacks our participants described.

Platforms could also offer safer exposure modes to enable increased sales to good-faith buyers. Some systems in prior work such as Predictive Response Optimization train machine learning algorithms to detect online social-network abuse [73]. Future work could explore adapting these systems to flag potentially threatening buyers for MBOs, allowing sellers to select which buyers they interact with. Some platforms serving MBs such as Reverb and Kickstarter already allow sellers to set operational terms and delivery timelines. If implemented well, such systems could limit a MBO's exposure to threats while empowering them to manage the growth of their business even in the face of interpersonal abuse [26].

7.2.2 Management of Coordinated Attacks

Throughout our study, MBOs discussed experiences of coordinated attacks and a desire for better tools that could be developed in future work. Payment processors identify certain patterns of mass payment-card fraud, but allow little room for nuance in who the perpetrator is. High volumes of chargebacks currently result in a seller being labeled as fraudulent, leading to suspension of a seller's account. But our participants report that buyers may weaponize these algorithms to purposefully trigger seller suspension. Future work may offer improved pathways for disputing a fraud-based suspension, or combine fraud detection with existing methods for detecting cross-platform coordinated online attacks [63].

As bad actors follow sellers across platforms (e.g., leaving negative reviews on Google maps, toxic comments on Instagram, and chargeback campaigns on Etsy), platforms could also investigate knowledge-sharing, such as creating cross-platform blocklists of harmful users [34] and seller support networks [48]. Contemporary enterprise tools use machine learning to offer threat intelligence that identifies cyberattack patterns in the wild and automates notification to risk-based cyber defense systems [12]. Services hosting MBOs could model coordinated outsider attacks and notify MBOs before they are under attack. In addition, the research community could conduct speculative participatory design studies with online sellers subject to personal abuse to identify the most helpful mechanisms for reducing the load of these attacks, and develop guides to avoid cross-platform effects [40].

7.2.3 Seller Protections

Prior work on technical help desks has recognized the need for entrepreneurial support [35], but our findings highlight specific, unaddressed attacks. Unlike gig workers who often feel micromanaged by restrictive algorithms [49], the sellers we interviewed faced the opposite issue: platform neglect. Rather than suffering from intrusive control, interviewed MBOs felt exposed by buyer-protection policies that bad-faith actors weaponized against them. To address this, platforms could leverage their role as intermediaries to balance seller stability with buyer retention. For example, a 'trusted seller' program could allow MBOs to set their own service-level agreements for delivery and communication, replacing opaque, platform-wide metrics with clear, manageable expectations. As noted, some existing platforms that serve segments of the MBO population allow them to define their own service-level agreements (SLAs) for response and delivery times, tailored to their specific business scale.

Furthermore, platforms should improve complaint resolution and content moderation tools to protect sellers from irrelevant or abusive reviews, as interviewees described reviews unrelated to product quality that were intended solely to harass sellers. Implementing automated filters could ensure reviews remain actionable and professional. Beyond technical fixes, there is a clear need for emotional and psychological validation of the fraud and harassment sellers face. By acknowledging that MBOs are individuals in precarious positions, platforms can move toward a 'design for safety' model that offers the same care-work benefits currently found in informal support communities like Reddit [69].

8 Conclusion

We have provided the first in-depth investigation of harms impacting at-risk MBs. Through a two-part study, including a review of 38 consultations of at-risk MBOs subject to insider harms, and semi-structured interviews with 16 MBOs, we showed that insider threats are common, often driven by limited resources and personal safety risks that made setting strict access boundaries difficult. We also highlighted how MBOs incurred financial and psychological harms attempting to satisfy buyer-centered platform standards imposed on them. We concluded our work by proposing tools and governance mechanisms to better protect at-risk MBOs.

Acknowledgments

We thank the reviewers of our paper for their insightful comments and suggestions. We also thank all our participants for sharing their stories with us to improve the safety of eCommerce and marketing platforms. This research was supported in part by NSF Awards 452614, and a Google Cyber Award.

Ethical Considerations

We interviewed at-risk micro-business owners about the harms they face. While we revealed crucial insights into attacks, coping mechanisms, and platform-based obstacles, we recognized the ethical implications of our work.

Our study focused on at-risk users and potentially traumatic experiences of online harm. This creates several risks, including the possibility of distress and re-traumatization for participants, breach of confidentiality, vicarious trauma, and escalation of ongoing abuse. To address this, we incorporated several precautions following the guidelines of conducting safe at-risk user research [4, 10].

As our study involved human subjects, we got approval from relevant institutional review boards (IRBs) for all study procedures, including our transcript analysis, interview recruitment process, interview procedure, and data security practices.

In line with Bellini et al. [10], we used sources of lower-risk data to augment our findings, namely, existing case transcripts of a technology abuse clinic. While insightful, this was insufficient for understanding the platform-based obstacles that micro-business owners face when dealing with online attacks. Thus, we deemed it necessary to conduct semi-structured interviews that focused on deepening our understanding of micro-business owners' lived experiences.

Study participants. Prior to each interview, we carefully explained the purpose of our study, possible risks to participants, and how collected data will be securely stored and used. We emphasized that participants may stop the interview at any time, or skip any questions that made them uncomfortable or distressed. To mitigate re-traumatization, we avoided potentially triggering words in our guiding questions and follow ups. Only after receiving consent from the participant, did we continue each interview. To ensure participants received benefit from participating in research, we provided compensation and offered our final manuscript as a resource for furthering their awareness of online harms.

After each interview, we informed participants of next steps, and linked resources to communicate any concerns. We carefully redacted personally identifiable information about the participant or their businesses from transcripts, and only referred to them by a unique identifier throughout our analysis and in this paper (i.e., P1-P16). We maintained strict access control to ensure any data from our study was only accessible by the authors on IRB-approved secure storage platforms.

Researchers. As a research team we aspire to support at-risk individuals through our work. However, user studies on sensitive topics like interpersonal abuse and online hate can risk vicarious trauma for researchers [10]. Two members of the research team are trained in trauma-informed care and another two have expertise on working with at-risk groups. Therefore, all authors enforced self-care procedures, and took frequent breaks during coding and analysis. Additionally, researchers conducted a maximum of two interviews a day.

Users of eCommerce platforms. Our study discusses experiences of online attacks, platform features that enable them, and why MBOs struggle in defending against them. We recognize that an adversarial user of an eCommerce platform may leverage these discussions to conduct additional harm or mount new attacks on business owners. Therefore, we withhold specific details of how attacks can be conducted , and present strategies for addressing the systematic pressures and platform deficiencies reported by participants.

Open Science

Our interviews involved discussions of sensitive experiences of harm by at-risk business owners, and included potentially identifiable information regarding their businesses. In working with our IRB and the consent process for our participants, we promised confidential storage of all interview data.

In consideration of these constraints, we do not share our coded interview transcripts as an artifact at this time. For researchers interested in working with our data, we will provide a de-identified version of our transcript data on a case-by-case basis. Nevertheless, we provide our full codebook, interview protocol, and recruitment materials (call for participation, recruitment flyer, and consent form) as artifacts at: https://doi.org/10.5281/zenodo.20330076.

References

[1] Etsy Seller Handbook, 2024. Accessed: 2025-09-09. URL: https://www.etsy.com/seller-handbook.

[2] Christina Anastasia. Exploring definitions of small business and why it is so difficult. *Journal of Management Policy and Practice*, 16(4):88, 2015.

[3] Abhay Aneja, Michael Luca, and Oren Reshef. The benefits of revealing race: Evidence from minority-owned local businesses. *American Economic Review*, 115(2):660–89, February 2025.

[4] Michael Bailey, David Dittrich, Erin Kenneally, and Doug Maughan. The menlo report. *IEEE Security & Privacy*, 2012.

[5] Bailey, Daniel V. and Munyendo, Collins W. and Dyer, Hunter A. and Grant, Miles and Markert, Philipp and Aviv, Adam J. "Someone Definitely Used 0000": Strategies, Performance, and User Perception of Novice Smartphone-Unlock PIN-Guessers. In *European Symposium on Usable Security*, EuroUSEC '23, Copenhagen, Denmark, October 2023. ACM.

[6] Catherine Barwulor, Allison McDonald, Eszter Hargittai, and Elissa M. Redmiles. "disadvantaged in the american-dominated internet": Sex, work, and technology. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, CHI '21, New York, NY, USA, 2021. Association for Computing Machinery.

[7] Thomas Baumer, Tobias Reittinger, Sascha Kern, and Günther Pernul. Digital Nudges for Access Reviews: Guiding Deciders to Revoke Excessive Authorizations. In *Twentieth Symposium on Usable Privacy and Security (SOUPS 2024)*, Philadelphia, PA, August 2024. USENIX Association.

[8] Rosanna Bellini. Paying the Price: When Intimate Partners Use Technology for Financial Harm. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, CHI '23, New York, NY, USA, April 2023. Association for Computing Machinery.

[9] Rosanna Bellini, Kevin Lee, Megan A Brown, Jeremy Shaffer, Rasika Bhalerao, and Thomas Ristenpart. The Digital-Safety Risks of Financial Technologies for Survivors of Intimate Partner Violence. In *USENIX'23 Security Symposium*, 2023.

[10] 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 *2024 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2024.

[11] Katya Borgos-Rodriguez and Anne Marie Piper. Understanding Participation among Disabled Creators in Online Marketplaces. *Proc. ACM Hum.-Comput. Interact.*, 7(CSCW2), October 2023.

[12] Xander Bouwman, Victor Le Pochat, Pawel Foremski, Tom Van Goethem, Carlos H Gañán, Giovane CM Moura, Samaneh Tajalizadehkhoob, Wouter Joosen, and Michel Van Eeten. Helping hands: Measuring the impact of a large threat intelligence sharing community. In *31st USENIX Security Symposium (USENIX Security 22)*, 2022.

[13] Virginia Braun and Victoria Clarke. Reflecting on reflexive thematic analysis. *Qualitative research in sport, exercise and health*, 11(4):589–597, 2019.

[14] Marko Cabric. *Corporate security management: Challenges, risks, and strategies*. Butterworth-Heinemann, 2015.

[15] Gabrielle Carpenter. What percentage of businesses are small businesses? Online (NAWBO Expert Reviews), May 2024. Accessed: September 4, 2025. URL: https://nawbo.org/expert-reviews/blog/percentage-of-small-businesses/.

[16] Kameri Christy, Tanice Welter, Kelly Dundon, Valandra, and Ambra Bruce. Economic abuse: A subtle but common form of power and control. *Journal of Interpersonal Violence*, 37(1-2):NP473–NP499, 2022.

[17] Joshua J Daspit, Corey J Fox, and S Kyle Findley. Entrepreneurial mindset: An integrated definition, a review of current insights, and directions for future research. *Journal of Small Business Management*, 61(1):12–44, 2023.

[18] Guy Davidov. Who is a worker? *Industrial Law Journal*, 34(1):57–71, 2005.

[19] Florian M. Farke, Lennart Lorenz, Theodor Schnitzler, Philipp Markert, and Markus Dürmuth. "You still use the password after all" – exploring FIDO2 security keys in a small company. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*. USENIX Association, August 2020.

[20] Stephanie Ferguson Melhorn, Makinizi Hoover, and Isabella Lucy. Small business data center. https://www.uschamber.com/small-business/small-business-data-center, 2025. [Accessed 30-06-2025].

[21] John C Flanagan. The Critical Incident Technique. *Psychological Bulletin*, pages 1–33, 1954.

[22] 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*, 2018.

[23] 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.

[24] Camille Harris, Amber Gayle Johnson, Sadie Palmer, Diyi Yang, and Amy Bruckman. "honestly, i think tiktok has a vendetta against black creators": Understanding black content creator experiences on tiktok. *Proc. ACM Hum.-Comput. Interact.*, 7(CSCW2), October 2023.

[25] Sharon Heung, Lucy Jiang, Shiri Azenkot, and Aditya Vashistha. “vulnerable, victimized, and objectified”: Understanding ableist hate and harassment experienced by disabled content creators on social media. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*, pages 1–19, 2024.

[26] Sharon Heung, Lucy Jiang, Shiri Azenkot, and Aditya Vashistha. "Ignorance is not Bliss": Designing Personalized Moderation to Address Ableist Hate on Social Media. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*, CHI '25, pages 1–18, New York, NY, USA, April 2025. Association for Computing Machinery.

[27] Ivan Homoliak, Flavio Toffalini, Juan Guarnizo, Yuval Elovici, and Martín Ochoa. Insight into insiders and it: A survey of insider threat taxonomies, analysis, modeling, and countermeasures. *ACM Computing Surveys*, 52(2):1–40, 2019.

[28] Jane Hsieh, Oluwatobi Adisa, Sachi Bafna, and Haiyi Zhu. Designing Individualized Policy and Technology Interventions to Improve Gig Work Conditions. In *Proceedings of the 2nd Annual Meeting of the Symposium on Human-Computer Interaction for Work*, CHIWORK '23, New York, NY, USA, September 2023. Association for Computing Machinery.

[29] Nicolas Huaman, Bennet von Skarczinski, Christian Stransky, Dominik Wermke, Yasemin Acar, Arne Dreißigacker, and Sascha Fahl. A Large-Scale interview study on information security in and attacks against small and medium-sized enterprises. In *30th USENIX Security Symposium (USENIX Security 21)*. USENIX Association, August 2021.

[30] Jessica Huang, Ning F Ma, Veronica A Rivera, Tabreek Somani, Patrick Yung Kang Lee, Joanna Mcgrenere, and Dongwook Yoon. Design tensions in online freelancing platforms: Using speculative participatory design to support freelancers' relationships with clients. *Proceedings of the ACM on Human-Computer Interaction*, 8(CSCW1), 2024.

[31] Lei Huang, Weijiang Yu, Weitao Ma, Weihong Zhong, Zhangyin Feng, Haotian Wang, Qianglong Chen, Weihua Peng, Xiaocheng Feng, Bing Qin, et al. A survey on hallucination in large language models: Principles, taxonomy, challenges, and open questions. *ACM Transactions on Information Systems*, 43(2).

[32] Julie Hui, Kristin Seefeldt, Christie Baer, Lutalo Sanifu, Aaron Jackson, and Tawanna R. Dillahunt. Community tech workers: Scaffolding digital engagement among underserved minority businesses. *Proc. ACM Hum.-Comput. Interact.*, 7(CSCW2), October 2023.

[33] Wiebke Hutiri, Orestis Papakyriakopoulos, and Alice Xiang. Not my voice! a taxonomy of ethical and safety harms of speech generators. In *Proceedings of the 2024 ACM Conference on Fairness, Accountability, and Transparency*, FAccT '24, New York, NY, USA, 2024. Association for Computing Machinery.

[34] Shagun Jhaver, Sucheta Ghoshal, Amy Bruckman, and Eric Gilbert. Online harassment and content moderation: The case of blocklists. *ACM Trans. Comput.-Hum. Interact.*, 25(2), March 2018.

[35] Yasmine Kotturi, Herman T Johnson, Michael Skirpan, Sarah E Fox, Jeffrey P Bigham, and Amy Pavel. Tech help desk: Support for local entrepreneurs addressing the long tail of computing challenges. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, CHI '22, New York, NY, USA, 2022. Association for Computing Machinery.

[36] Klaus Krippendorff. *Content analysis: An introduction to its methodology*. Sage publications, 2018.

[37] Costas Lambrinoudakis, Stefanos Gritzalis, Fredj Dridi, and Günther Pernul. Security requirements for e-government services: a methodological approach for developing a common pki-based security policy. *Computer communications*, 26(16), 2003.

[38] Leona Lassak, Philipp Markert, Maximilian Golla, Elizabeth Stobert, and Markus Dürmuth. A comparative long-term study of fallback authentication schemes. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*, 2024.

[39] Karen Levy and Bruce Schneier. Privacy threats in intimate relationships. *Journal of Cybersecurity*, 6(1), 2020.

[40] Hajin Lim, Lisa Kakonge, Yaxin Hu, Lyn Turkstra, Melissa Duff, Catalina Toma, and Bilge Mutlu. So, i can feel normal: Participatory design for accessible social media sites for individuals with traumatic brain injury. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, CHI '23, New York, NY, USA, 2023. Association for Computing Machinery.

[41] Robert N Lussier and Matthew C Sonfield. “Micro” versus “small” family businesses: a multinational analysis. *Journal of Small Business and Enterprise Development*, 22(3):380–396, 2015.

[42] Ning F. Ma, Veronica A. Rivera, Zheng Yao, and Dongwook Yoon. “Brush it Off”: How Women Workers Manage and Cope with Bias and Harassment in Gender-agnostic Gig Platforms. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*,

CHI '22, New York, NY, USA, April 2022. Association for Computing Machinery.

[43] Philipp Markert, Theodor Schnitzler, Maximilian Golla, and Markus Dürmuth. " as soon as it's a risk, i want to require {MFA"}: How administrators configure risk-based authentication. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*, 2022.

[44] Diogo Marques, Tiago Guerreiro, Luis Carriço, Ivan Beschastnikh, and Konstantin Beznosov. Vulnerability & Blame: Making Sense of Unauthorized Access to Smartphones. In *ACM Conference on Human Factors in Computing Systems*, CHI '19, Glasgow, Scotland, United Kingdom, April 2019. ACM.

[45] Diogo Marques, Ildar Muslukhov, Tiago Guerreiro, Luís Carriço, and Konstantin Beznosov. Snooping on Mobile Phones: Prevalence and Trends. In *Symposium on Usable Privacy and Security*, SOUPS '16, pages 159–174, Denver, Colorado, USA, July 2016. USENIX.

[46] Tara Matthews, Kerwell Liao, Anna Turner, Marianne Berkovich, Robert Reeder, and Sunny Consolvo. " she'll just grab any device that's closer" a study of everyday device & account sharing in households. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, pages 5921–5932, 2016.

[47] Allison McDonald, Catherine Barwulor, Michelle L Mazurek, Florian Schaub, and Elissa M Redmiles. " it's stressful having all these phones": Investigating sex workers' safety goals, risks, and practices online. In *30th USENIX Security Symposium (USENIX Security 21)*, pages 375–392, 2021.

[48] Colten Meisner. Networked responses to networked harassment? creators' coordinated management of "hate raids" on twitch. *Social Media+ Society*, 9(2):20563051231179696, 2023.

[49] Mareike Mohlmann and Lior Zalmanson. Hands on the wheel: Navigating algorithmic management and uber drivers' autonomy. In *Proceedings of the International Conference on Information Systems (ICIS 2017)*, ICIS '17', 2017.

[50] Sarah Myers West. Censored, suspended, shadowbanned: User interpretations of content moderation on social media platforms. *New Media & Society*, 20(11):4366–4383, 2018.

[51] Richard E Nisbett and Timothy D Wilson. The halo effect: Evidence for unconscious alteration of judgments. *Journal of personality and social psychology*, 35(4):250, 1977.

[52] Borke Obada-Obieh, Yue Huang, and Konstantin Beznosov. The Burden of Ending Online Account Sharing. In *ACM Conference on Human Factors in Computing Systems*, CHI '20, pages 503:1–503:13, Honolulu, Hawaii, USA, April 2020. ACM.

[53] Cheul Young Park, Cori Faklaris, Siyan Zhao, Alex Sciuto, Laura Dabbish, and Jason Hong. Share and share alike? an exploration of secure behaviors in romantic relationships. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*, 2018.

[54] Celia Paulsen and Patricia Toth. Small Business Information Security: The Fundamentals, 2016. NISTIR 7621r1. URL: https://nvlpubs.nist.gov/nistpubs/ir/2016/nist.ir.7621r1.pdf.

[55] Will B Payne. Review bombing the platformed city: Contested political speech in online local reviews. *Big Data & Society*, 11(3):20539517241275879, 2024. doi:10.1177/20539517241275879.

[56] Reddit Help. What is karma?, 2025. Accessed: 2026-02-04. URL: https://support.reddithelp.com/hc/en-us/articles/204511829-What-is-karma.

[57] Patrawat Samermit, Anna Turner, Patrick Gage Kelley, Tara Matthews, Vanessia Wu, Sunny Consolvo, and Kurt Thomas. {"Millions} of people are watching {you"}: Understanding the {Digital-Safety} needs and practices of creators. In *32nd USENIX Security Symposium (USENIX Security 23)*, pages 5629–5645, 2023.

[58] Lisa J Servon. Microenterprise development in the united states: Current challenges and new directions. *Economic Development Quarterly*, 20(4):351–367, 2006.

[59] Caoyang Shen and Oliver L. Haimson. The virtual jail: Content moderation challenges faced by chinese queer content creators on douyin. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*, CHI '25, New York, NY, USA, 2025. Association for Computing Machinery.

[60] Yoonseock Son, Kaitlin D Wowak, and Corey M Angst. Does Greater Visibility Benefit Minority Businesses? Evidence from an Online Review Platform. *Production and Operations Management*, 34(4), April 2025. Publisher: SAGE Publications.

[61] Yunpeng Song, Cori Faklaris, Zhongmin Cai, Jason I. Hong, and Laura Dabbish. Normal and Easy: Account Sharing Practices in the Workplace. In *ACM Conference on Computer-Supported Cooperative Work and Social Computing*, CSCW '19, Austin, Texas, USA, November 2019. ACM.

[62] Stack Overflow. What is reputation? how do i earn (and lose) it?, 2026. Accessed: 2026-02-04. URL: https://stackoverflow.com/help/whats-reputation.

[63] Gianluca Stringhini, Pierre Mourlanne, Gregoire Jacob, Manuel Egele, Christopher Kruegel, and Giovanni Vigna. EVILCOHORT: Detecting communities of malicious accounts on online services. In *24th USENIX Security Symposium (USENIX Security 15)*, pages 563–578, Washington, D.C., August 2015. USENIX Association.

[64] Arnesh Telukdarie, Thabile Dube, Pretty Matjuta, and Simon Philbin. The opportunities and challenges of digitalization for SME's. *Procedia Computer Science*, 217:689–698, 2023.

[65] Mary Theofanos, Simson Garfinkel, and Yee-Yin Choong. Secure and Usable Enterprise Authentication: Lessons from the Field. *IEEE Security & Privacy*, 14(5):14–21, September 2016.

[66] Kurt Thomas, Devdatta Akhawe, Michael Bailey, Dan Boneh, Elie Bursztein, Sunny Consolvo, Nicola Dell, Zakir Durumeric, Patrick Gage Kelley, Deepak Kumar, et al. Sok: Hate, harassment, and the changing landscape of online abuse. In *2021 IEEE symposium on security and privacy (SP)*, pages 247–267. IEEE, 2021.

[67] TikTok. Creator Identity Verification, 2024. Accessed: 2025-09-09. URL: https://seller-us.tiktok.com/university/essay?knowledge_id=8182993140467499.

[68] TikTok. How To Use User Management, 2024. Accessed: 2025-09-09. URL: https://seller-us.tiktok.com/university/essay?knowledge_id=6837907030279937.

[69] 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*, New Orleans LA USA, April 2022. ACM.

[70] Kristen Vaccaro, Christian Sandvig, and Karrie Karahalios. "at the end of the day facebook does what itwants": How users experience contesting algorithmic content moderation. *Proc. ACM Hum.-Comput. Interact.*, 4(CSCW2), October 2020. doi:10.1145/3415238.

[71] 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)*. IEEE, 2022.

[72] Gianna Williams, Natalie Chen, Michael Ann DeVito, and Alexandra To. Why Can't Black Women Just Be?: Black Femme Content Creators Navigating Algorithmic Monoliths. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*, CHI '25, New York, NY, USA, April 2025. Association for Computing Machinery.

[73] Garrett Wilson, Geoffrey Goh, Yan Jiang, Ajay Gupta, Jiaxuan Wang, David Freeman, and Francesco Dinuzzo. Predictive Response Optimization: Using Reinforcement Learning to Fight Online Social Network Abuse. In *Proceedings of the 34th USENIX Security Symposium (USENIX Security 2025)*, Santa Clara, CA, USA, 2025. USENIX Association.

[74] Flynn Wolf, Adam J. Aviv, and Ravi Kuber. Security obstacles and motivations for small businesses from a CISO's perspective. In *30th USENIX Security Symposium (USENIX Security 21)*, August 2021.

[75] Ruiyun Xu, Yue (Katherine) Feng, and Hailiang Chen. Chatgpt vs. google: A comparative study of search performance and user experience. https://ssrn.com/abstract=4498671, 2023. [Accessed 12-06-2025].

[76] Ratna Yudhiyati, Afrida Putritama, and Diana Rahmawati. What small businesses in developing country think of cybersecurity risks in the digital age: Indonesian case. *Journal of Information, Communication and Ethics in Society*, 19(4):446–462, 2021.

A Appendix

A.1 Case Search Analysis

We were provided access to 623 cases of consultations with survivors of interpersonal abuse. To find cases in which MBs are discussed, we performed keyword searches using the keywords displayed in Table 3. Searches were performed in a secure online environment. Once results were returned, two members of the research team manually examined the document, determining if the discussion included mentions of harms impacting or targeted at a business the survivor owned or operated in. If such discussions were being had, the document was labeled as relevant. A total of 38 (6% of total cases in the dataset) relevant cases were identified through this search method.

A.2 Interview protocol and qualitative codebook

Table 4 displays our interview theme-to-code mapping. The full codebook is provided in the online artifacts.

Type	Keywords
Actions	Purchase[s], Buy, Bid, Sell, Resource[s, ing], Sale, Steal, Fake, Report
Institution	Business, Freelancer, Contractor, Company, Bank, Brand, IRS
Brand	Bank, Marketplace, Amazon Seller/Store, Shopift, TikTok Shop, Etsy, Taskrabbit, Facebook Marketplace, Big Cartl
Financial Products	Damage Insurance, Loan [s], Invest, Fund, Accounting, Margin, Profit, Turnover, Expenses, Income, Loss
Business Personnel	Customer, Colleague, Employ[ee, er], Boss
Item	Product, Credit, Store[s, front], Shop[s, front]

Table 3: List of keywords used to search through the consultation files with survivors of interpersonal abuse in order to find cases in which harms to MBOs were discussed.

B Interview Protocol

Thank you for taking the time to participate in our study!
In this work, we're exploring how technology impacts small and micro-businesses run by individuals at greater risk of harm, particularly in facing online attacks. We want to understand the types of harm businesses like yours face, how [platform-of-use] may help or hinder these attacks, and your suggestions for improving digital safety for all. Were you able to review the information sheet and consent form? Do you have any questions before we begin?

This session will take about 60 minutes. We'll be asking 10 questions about your experiences as a small business owner using technology and online services. We'll also discuss your business, any experiences of challenging financial situations caused by these technologies, and recovery paths you've explored or would like to see—this should take about 50 minutes. Finally, we'll spend 5 minutes going over the next steps. We'll discuss your experiences with digital attacks, which may be distressing to you. The risk is no greater than discussing it with a trusted friend or professional. If at any point you feel uncomfortable, you're free to pause, take a break, or stop.

Do we have your permission to take notes in this session? And audio record the session?

B.1 Introduction

Purpose: Understanding the baseline functions of the business. To start, I'd like to know a little bit more about your business.

- Could you tell me a short history about your business, including your motivation behind starting the business, what you sell, how long you've been running/managing the business?
- So you mentioned that you use [online marketplace(s)] to conduct /advertise your business, how did you decide on using these marketplaces? *Prompt: benefits or restrictions of specific marketplaces, cost, 'just happened'*
- Okay, and do you use other online or digital platforms for promoting your business, or managing payments? Can you walk me through how that works? *Prompt: customized paid ads, square/cashApp*
- Are there any other uses of digital technologies in your business that you think we haven't covered? *Prompt: recruitment, reporting, online listings, search engine optimization*

B.2 Customer-interactions

Purpose: Understanding the (potential) starting points of attacks

- How would you summarize your online customer base? *Prompt: any demographics, online/offline, one-time purchasers vs subscribers*
- How do customers come to find out about your business? Can they contact you about services/products through this method? *Prompt: suggest common communication channels (e.g., direct messages, reviews)*
- How can customers leave feedback for you about your business online? What is the process for this helping shape your business? *Prompt: google reviews, product reviews, post, market analysis*

B.3 Attacks on business or self

Purpose: Identifying the forms of attacks faced by business owners.

Okay, I'm just going to shift the attention to when someone associated with your business intended to cause harm to your business; you can speak about either customers, ex-employees, or business partners. By "partner," we mean either a co-owner or significant collaborator that helps your business function. By harm, you could think about any behavior or pattern of behavior that causes damage to your personal reputation, your branding, how your business functions, or your confidence to run your business as usual.

- Can you think back to a challenging time involving someone directly associated with your business? *Prompt: dependent on account provided by participant*
- Have there been any occasions when you felt like someone associated with your business targeted you in a way that was intended to cause you harm? How did they do this? What was the impact on your business? *Prompt: persons involved, type of attack*
- Can you think of a time where someone impersonated you/smeared your reputation online/attempted a business takeover/maliciously reported you/coerced you financially/shared private information 'doxxed' you*? *Prompt: persons involved, attack vectors, steps to mitigate harm*
- Summarize the participant account from the previous question. When this happened, what kinds of steps did you take in response to this? *Prompt: take steps to mitigate harm, ask a friend/family member*
- Did you send a report to the platform about this? How satisfied were you with their response? *Prompt: timeline, lack of communication*

B.4 Suggestions for Business-Relevant Platforms

Purpose: Identifying what business owners would have wanted to help mitigate harm. Now that we've talked about the different ways you've faced harm with your business, I'd like to chat a little bit about what you think platforms could have done or should do in the future to help out scenarios like the ones you've described.

- *Answer dependent*. Let's think back to account provided by participant, can you think of any specific things the platforms you use could have done to help you as a business owner in dealing with the individual's actions in the moment? *Prompt: which platforms, why it'd be helpful, impact on interviewer*
- If participant is struggling with coming up with particular things For instance, are there specific actions the platform could have provided that would have helped you prevent the individual from contacting you? *Prompt: which platforms, why it'd be helpful, impact on interviewer*
- *Answer dependent.* To expand on that, was there anything the platform could have done to better support you as you tried to recover from the challenging circumstance? *Prompt improving communication, financial help, regaining access, filing reports*

Themes
Guilt, Shame, & Self-Doubt
Business harms mental health
Fear shapes protective behavior
Compromises are challenging to discuss (shame)
Giving up on solutions
Hypervigilance
Double Edge Sword of Visibility
Hypervisibility
Visibility and customer reach challenges
Credibility and trust
Pressure to meet large-business standards
Trust in Insiders
Insider trust leading to harm
Insider attacks not recognized
Seller safety negligence
Power Dynamics & Control
Punishment over reward
Customer policy weaponization
Exploitative platforms
Difficult incident response
Platforms hide harms
No platform intervention
Minimal faith in platform
Platform norm's influence on customer behavior
Lack of control
Misc
Identity-business entanglement
Wearing multiple hats
Harm resolution overhead
Values-based customer interference
Descriptive Codes
Features & Attempts at Protection
Peer support networks
Coping Mechanisms
System folk theories
Features of platforms
Paid security services
Harms
Mention of attacks experienced
No legal support
Platform usability issues

Table 4: Condensed codebook used to analyze the interviews conducted with small business owners.