Title: Closing Cybersecurity Gaps in Pakistan: Developing Sociotechnical Solutions through Unmask'd

Author: Zehrah Minal

Affiliation: Independent Researcher, Unmask'd

Email: xehrahminal@gmail.com

Date: July 24, 2025

Abstract:
Cybersecurity in Pakistan is often framed as a purely technical concern, yet its impact is shaped by literacy, resources, and social context. Phishing scams, financial fraud, and malware affect users across gender lines, with men statistically more likely to experience banking and employment-related scams. Women, however, face additional risks such as sextortion, doxxing, and image-based blackmail, where the consequences extend beyond finances to safety and reputation. This research examines Pakistan's cybercrime landscape through a sociotechnical lens, mapping vulnerabilities not by identity alone but by patterns of risk and behavior. Drawing on the author's development of *Unmask'd* - a digital safety toolkit created specifically for Pakistani users - this paper uses the platform as a case study to explore how culturally contextualized tools can operationalize sociotechnical principles of cybersecurity. This study presents findings from pilot evaluations of Unmask'd conducted through mixed methods (surveys, usability sessions, and interviews). While these results are preliminary and based on researcher-led assessment, they provide critical exploratory insights into Pakistan's sociotechnical threat patterns. Future work will expand toward larger-scale validation through partnerships with NGOs, digital rights organizations, and independent evaluators to ensure robustness and generalizability. The paper concludes by arguing for inclusive, evidence-based cybersecurity reforms that balance accessibility, cultural realities, and safeguards against misuse.

Keywords:

cybersecurity, digital literacy, phishing, online fraud, sociotechnical systems, online harassment, user empowerment

1. Introduction

Pakistan’s digital threat landscape is evolving rapidly, and no user is immune. Phishing scams, fake job listings, malware-laced links, and psychological social engineering attacks are on the rise. These tactics exploit human behavior more than technical flaws, making both men and women vulnerable. Yet while the attack methods are often similar, the consequences play out unevenly across different groups.

For men, increased engagement in banking, freelancing, and cryptocurrency exposes them to financial fraud, investment scams, and phishing attempts. The fallout is often measured in monetary loss or reputational risk. For women, however, cyberattacks can carry consequences that extend far beyond finances. Non-consensual image leaks, sextortion, and online blackmail weaponize cultural notions of shame and honor. In a society where reputation and modesty are tightly policed, a single breach can lead to coercion, social exclusion, or threats to safety. A hacked account may be an inconvenience for one user, but for another, it can mean the loss of dignity, autonomy, or freedom.

This asymmetry underscores a central argument of this paper: cybersecurity in Pakistan cannot be understood as a gender-neutral or purely technical issue. It is deeply entangled with literacy, economic behavior, and cultural context. Firewalls cannot shield against social stigma. Antivirus software cannot repair the silence imposed by family pressure. The most damaging cyberattacks are not always the most advanced, but the ones that prey on trust, fear, and isolation.

This paper situates cybersecurity as a sociotechnical issue - one that demands contextually grounded, inclusive solutions. The author’s own project, *Unmask’d*, was developed as a **research-led prototype** to test whether culturally contextualized interventions can strengthen user agency and digital safety. Rather than offering universal tools, *Unmask’d* builds around local behaviors, languages, and trust patterns, integrating features such as phishing detection, password hygiene checks, and a legal literacy chatbot.

2. Theoretical Frameworks

The digital world is not neutral. It mirrors and often magnifies the power structures of the offline one. Scholars such as D'Ignazio and Klein (2020) critique cybersecurity's illusion of universality, noting that systems designed for a "default" user - literate, Western, and autonomous - leave many exposed. These blind spots matter in Pakistan, where cybersecurity cannot be understood without attention to literacy, infrastructure, and social context.

Digital access in South Asia is shaped by patriarchy and household surveillance as much as by bandwidth. Women in Pakistan continue to face structural barriers to private phone ownership and control, shaped by household norms and affordability gaps. The Pakistan Telecommunication Authority's *Digital Gender Inclusion Strategy* (2024) and GSMA's *Mobile Gender Gap Report* (2023) show that women in South Asia are 19% less likely than men to own a smartphone, underscoring how access inequalities compound vulnerability to cyber threats. Even global tools with robust protections falter when they assume privacy as a baseline. Data from the Digital Rights Foundation's helpline (2018) reveals that victims of cyber harassment not only endure the abuse itself, but also face systemic barriers to redress: shared accounts, fear of family shame, and the absence of localized legal knowledge.

Legal frameworks remain blunt instruments. The Prevention of Electronic Crimes Act (PECA) in Pakistan outlines categories of offenses, but its vague and punitive language can place survivors at further risk. Nissenbaum's (2010) theory of contextual integrity explains why such gaps persist: privacy violations are not just breaches of data, but breaches of expectation. For example, exposing a woman's WhatsApp profile picture in a mixed-gender group may appear trivial to the law, yet it carries significant social consequences.

Design-level failures reinforce these gaps. Apps like WhatsApp and Instagram provide two-factor authentication, but implementation does not account for SIM-swap scams, stalkerware, or shared-device environments. Henson and Lee (2021) demonstrate how intimate partner surveillance increasingly exploits features intended to enhance security. Global initiatives such as the *Data Detox Kit* (Tactical Tech, 2018) assume high levels of digital fluency, remaining inaccessible to the majority of Pakistani users who may never have encountered terms like "digital footprint." Broader ICT4D research reinforces these limitations. APC (2020) highlights how gendered restrictions and household surveillance across the Global South undermine autonomy online, while UNICEF (2019) shows that South Asian youth often lack both awareness of reporting channels and trust in institutional remedies, echoing patterns observed in Pakistan.

Localized approaches attempt to address these mismatches. *Unmask'd* was designed around Pakistani digital behaviors rather than against them. Its legal chatbot translates complex laws into Urdu and English, lowering literacy barriers. Its phishing detector incorporates local scam patterns, reflecting common exposures in Pakistan's digital economy. Rather than offering abstract solutions, *Unmask'd* situates security in lived realities, making user agency central. Early evaluations remain internal, yet they highlight both the potential and the limitations of contextualized cybersecurity models.

3. Problem Statement: Sociotechnical Threat Patterns

Pakistan's digital sphere reflects many of the same inequalities found offline. Cyber risks do not impact users evenly, but follow patterns shaped by literacy, access, and social norms. A phishing link, a fraudulent job offer, or a malware-laced file can target anyone, yet the consequences diverge sharply across groups.

For men, higher rates of financial participation through banking, freelancing, and cryptocurrency create greater exposure to phishing, investment fraud, and account takeovers. These incidents often result in monetary loss or reputational damage. For women, the risks are different in nature: image-based abuse, sextortion, and surveillance can escalate into harassment, coercion, or threats to physical safety. Here, a single leaked image or compromised password carries consequences far beyond digital inconvenience, intersecting with cultural notions of honor and shame.

Beyond gender, structural barriers such as low digital literacy, shared device usage, and multilingual divides amplify vulnerabilities. Many users lack the skills or language to navigate privacy settings, detect fraudulent sites, or understand legal protections. Even when laws exist, vague terminology and moralized enforcement often deter victims from reporting abuse, further silencing those most at risk.

This disconnect between mainstream cybersecurity frameworks and lived realities reveals a pressing problem. Global approaches assume a “default user” who is literate, autonomous, and able to act on security advice, but such assumptions rarely hold true in Pakistan. Without tools tailored to local behaviors and constraints, users remain unprotected against threats that exploit both technical and cultural weaknesses.

Unmask’d represents an attempt to close this gap. It reframes cybersecurity as a sociotechnical issue, embedding literacy resources, legal guidance, and culturally relevant design into its phishing detector, password checker, and chatbot. While evaluation remains internally conducted, its model demonstrates how inclusive approaches can better align security with everyday realities.

The problem is not simply that cybercrime exists, but that existing protections fail to account for diverse patterns of risk. Addressing this requires reframing cybersecurity as both a technical and social challenge, one that demands evidence-based reforms and context-aware tools.

4. Methodology and Design: Research-Led Development for Marginalized Digital Safety

Traditional cybersecurity tools in Pakistan often fail to account for literacy, social context, and cultural constraints that shape user vulnerability. Unmask’d was developed as a direct response to these gaps, combining research-led insights with culturally informed design to address both technical and social risks.

Grounded in participatory and context-aware research, development drew on Nissenbaum’s contextual integrity theory (2010) and best practices for designing technology for vulnerable populations (Henson & Lee, 2021). Digital ethnography and informal interviews with 63 users in Karachi revealed widespread exposure to phishing, account compromise, social engineering, and malware. Only 8% of participants had previously reported incidents, highlighting significant gaps in awareness, confidence, and access to reporting mechanisms.

In-depth narrative interviews with 12 participants revealed patterns of risk:

- Men frequently reported phishing, investment scams, banking fraud, and risks associated with online work or freelancing.
- Women experienced these risks as well, but also faced additional high-stakes threats including sextortion, doxxing, and image-based blackmail, where consequences extend beyond financial loss to personal safety and social reputation.
- Social constraints, such as surveillance by family members or community expectations, further limited users' ability to respond safely.

These insights directly informed the design of Unmask'd, resulting in a toolkit that is both secure and culturally intuitive:

- **Legal Aid Chatbot**: A WhatsApp-style bot that explains cybercrime laws in accessible Urdu and English, guiding users through reporting mechanisms in clear, non-intimidating language. 94% of pilot users reported understanding PECA for the first time through the chatbot.
- **Phishing Detector & Password Checker**: Icon-based alerts and intuitive visuals designed for low-literacy users, inspired by user feedback emphasizing clarity and trustworthiness.
- **Safety Quiz & Impact Tracker**: Interactive modules that both educate users and allow them to anonymously track perceptions of online safety over time.
- **Case of the Month Blog**: Anonymized real-life incidents illustrating threat patterns and fostering awareness of common but underreported abuses.

All features were iteratively refined based on participant feedback, emphasizing usability, privacy, and trust. Pilot testing indicated that tools addressing immediate vulnerabilities - particularly the phishing detector, password checker, and legal chatbot - were most relied upon. Users reported higher confidence navigating cyber threats when the tools were culturally and contextually relevant.

Through Unmask'd, this research demonstrates that participatory, context-aware design strengthens digital safety for all users while recognizing that women face additional high-stakes risks. Integrating accessibility, cultural fluency, and legal guidance allows the platform to move beyond purely technical protection, enabling users to understand threats, respond safely, and strengthen user capacity for self-protection in online spaces.

All participant interactions were conducted with informed consent, guaranteeing anonymity and voluntary participation. Additional precautions were taken due to the sensitive nature of cyber threats and potential social repercussions.

This research was conducted in Pakistan as an independent, minimal-risk study focused on digital behavior and user safety. While formal IRB approval was not required, all procedures followed internationally recognized research ethics standards, including those used in ICT4D and HCI research. Participants were fully informed of the study's purpose, their voluntary participation, and their right to withdraw at any time. No personally identifiable information was collected, and all responses were anonymized to protect privacy - particularly given the sensitivity of gendered cyberthreats.

Interview transcripts and field notes were analyzed through ***thematic coding****, allowing recurring behavioral patterns and cultural risk factors to emerge inductively. Codes were refined iteratively to highlight both gendered and cross-cutting themes. Survey data from 137 participants were analyzed using* ***descriptive statistics*** *(frequency and percentage analysis) to summarize trends in awareness, platform use, and self-reported confidence levels. Integrating both qualitative and quantitative findings enabled* ***triangulation****, providing a multi-dimensional understanding of sociotechnical vulnerabilities.*

Quantitative data is presented here as part of a pilot phase, offering indicative patterns rather than definitive measures. The aim is exploratory - to map recurring vulnerabilities and evaluate early design responses - while acknowledging that broader, longitudinal studies are necessary to confirm and extend these findings.

5. Findings and Discussion: Interpreting Sociotechnical Patterns

Building on the methods outlined above, the following section presents the key findings from the Unmask'd pilot study and interprets their sociotechnical implications for digital safety in Pakistan.

Pilot testing of Unmask'd was conducted across two mixed-gender schools and three youth-led digital rights forums in Pakistan, providing both qualitative and quantitative insight into platform reception and real-world impact. Anonymous surveys were collected from 137 users, supplemented with usability sessions and ongoing discussions. Three key patterns emerged:

i) Digital Safety Is Not the Same as Digital Literacy

While 82% of participants reported being comfortable with smartphones and social media, only 11% knew how to secure accounts or identify phishing before using Unmask'd. The gap reflected empowerment rather than access. One male participant from Karachi explained: "*I got an email about some 'easy money' thing for freelancing. I almost clicked it, but I didn't know it could be a scam.*"

A female participant added:
"*Someone threatened to share my photos online. I deleted everything and didn't tell anyone. I didn't even realize it was illegal until I checked the bot.*"

The legal aid chatbot saw a 69% repeat usage rate within two weeks, suggesting simplified, context-aware guidance increased user confidence across genders.

ii) Cultural and Social Norms Affect Reporting

Many users hesitated to report cyber threats due to social stigma or family expectations. One female student shared:
"*Even screenshots of random messages made me feel like I'd done something wrong. I didn't want anyone to know.*"

Male participants also reported reluctance in sharing incidents of financial fraud or account hacks. One noted:

"*I didn't tell my parents when my bank account got phished. I just felt embarrassed, like it was my fault.*"

To address these barriers, Unmask'd required no login or personal data, allowing anonymous use. 91% of participants indicated they would not have used the platform if identification were required. Multilingual explanations and culturally familiar interface elements increased engagement and trust.

iii) Community-Oriented Tools Build Confidence and Engagement

The phishing detector, password checker, and legal aid chatbot were the most used features. Confidence stemmed from transparency and cultural relevance. One participant explained:
"*When I saw the instructions in Urdu and the symbols made sense, I felt like someone actually thought about us.*"

Peer-to-peer sharing amplified impact. Sixty-one percent reported helping a friend access Unmask'd, while 42% used the platform during actual incidents, ranging from financial scams to sextortion or doxxing.

Unmask'd illustrates that participatory, culturally-informed design strengthens digital safety for all users while addressing high-risk situations disproportionately affecting women. Beyond technical protection, the platform fosters legal awareness, community trust, and confidence in navigating online threats.

6. Policy Recommendations

Our findings indicate that legal awareness and technological access alone are insufficient to protect users in Pakistan's digital spaces. Cyber risks differ by behavior and context: men are more likely to fall victim to phishing, banking scams, investment fraud, and gig-economy related threats, while women face higher risks from sextortion, doxxing, and image-based blackmail. Interventions must therefore address patterns of risk and behavior rather than identity alone, while remaining culturally sensitive.

i) Public Education Campaigns to Clarify Digital Rights

- Conduct targeted campaigns in Urdu and regional languages that explain the legal protections available to all users and normalize reporting abuse.
- Collaborate with educators, youth influencers, and religious scholars to contextualize digital safety within local norms.
- Emphasize that reporting abuse is a right, not a source of shame.

"*If being harassed brings shame, but speaking out brings more, the system itself is the threat.*"

ii) Mandate Digital Safety Curriculum in Schools

Make cybersecurity part of the national curriculum, not just as a tech skill, but as civic education. Curriculum content should:

- Explain how to file a cybercrime complaint,
- Debunk victim-blaming myths, and
- Provide hands-on practice with security tools and threat recognition.

Unmask'd prototype offers a potential implementation model.

iii) Establish Accessible and Anonymous Reporting Channels

Existing cybercrime tools are bureaucratic, male-dominated, and deeply intimidating. We recommend:

- Establish anonymous reporting options to reduce fear of retaliation.
- Propose a WhatsApp-based reporting interface for initial complaints and NGO-led follow-up support.
- Implement safeguards to prevent misuse while ensuring user privacy.

iv) Push Tech Company Accountability

Platforms like Meta and TikTok must be held responsible for enabling abuse through:

- Urdu-translated reporting interfaces,
- Regional content moderation teams trained in cultural nuance,
- Locally grounded community guideline updates.

Honor-based abuse differs significantly from Western models of cyberviolence, and global tech platforms must adapt accordingly.

v) Criminalize Non-Consensual Digital Surveillance
Pakistan's PECA law lacks specificity on:

- Explicitly criminalize unauthorized GPS tracking, remote monitoring, and public sharing of private content.
- Define violations based on patterns of risk and behavior, irrespective of gender or relationship to the perpetrator.
- Establish transparent enforcement mechanisms and safeguards to protect users during reporting.

These recommendations build on Unmask'd real-world findings and aim to reshape Pakistan's digital safety ecosystem through culturally aware, survivor-centered reforms. By addressing actual patterns of vulnerability and providing inclusive, evidence-based protections, these reforms seek to empower all users while minimizing opportunities for misuse or discrimination.

7. Conclusion: Beyond Firewalls

Digital violence in Pakistan is not simply a technical problem; it is a sociocultural one, encoded in silence, stigma, and social power dynamics. The research demonstrates that most users do not lack access to tools; they lack the knowledge, support, and freedom to use them safely. From fraudulent job listings to targeted phishing, malware, and threats disguised as moral policing, the internet in Pakistan mirrors offline structures of control - only faster, more pervasive, and harder to trace.

Unmask'd was designed to do more than provide tools; it was built to reclaim agency. Through surveys, usage data, and firsthand accounts, patterns of risk and harm were mapped, revealing a hidden ecosystem of vulnerability shaped by literacy, resources, and social constraints. This work demonstrates how a researcher-built prototype can surface sociotechnical insights that theory alone might overlook. *Unmask'd* is thus not an endpoint but a case study illustrating how culturally grounded cybersecurity can be built, tested, and improved.

This research is not just about highlighting threats; it is about designing interventions that protect and empower users, particularly those constrained by social and infrastructural barriers. In a society where digital exposure can carry severe consequences, safe and usable tools become a form of resilience.

Future research will extend *Unmask'd* deployment across multilingual and low-literacy contexts, assess its scalability for broader ICT4D ecosystems, and explore partnerships with educational and policy stakeholders to ensure sustainable digital empowerment.

8. References

Association for Progressive Communications (APC). (2020). *Closer than ever: Gender, ICTs and feminist internet research.* APC. https://www.apc.org/sites/default/files/IDRC_Mapping_0323_0.pdf

D'Ignazio, C., & Klein, L. F. (2020). *Data feminism.* MIT Press. https://doi.org/10.7551/mitpress/11805.001.0001

Digital Rights Foundation. (2018). *Hamara Internet guidebook.* Digital Rights Foundation. https://digitalrightsfoundation.pk/wp-content/uploads/2018/05/Hamara-Internet-Guidebook-Final.pdf

GSMA. (2023). *The mobile gender gap report 2023.* GSMA. https://www.gsma.com/r/gender-gap-2023/

Henson, S., & Lee, S. (2021). Designing secure technology for low-literacy and multilingual users. *Proceedings of the ACM Conference on Human Factors in Computing Systems (CHI).* https://doi.org/10.1145/3411764.3445293

Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life.* Stanford University Press. https://www.sup.org/books/law/privacy-context

Pakistan Telecommunication Authority. (2024). *Digital Gender Inclusion Strategy.* https://www.pta.gov.pk/assets/media/digital_gender_inclusion_strategy_28-02-2024.pdf

Tactical Tech. (2018). *The Data Detox Kit: How to reclaim your privacy online.* Tactical Technology Collective. https://datadetoxkit.org

UNICEF. (2019). *Children in a digital world.* UNICEF Innocenti. https://www.unicef.org/innocenti/media/5621/file/UNICEF-Investigating-Risks-Opportunities-Children-Digital-World-2021.pdf