DRF

DigitalRightsFoundation

"KNOW YOUR RIGHTS"

2024

Digital Security Helpline Annual Report

About Digital Rights Foundation

Digital Rights Foundation (DRF) is a women-led, not-for-profit organization working since 2013 to advance digital rights and online freedoms across South Asia and the broader Global Majority. We advocate for inclusive, rights-respecting digital spaces by driving policy change through strategic engagement with relevant stakeholders. Our work focuses on making digital platforms and emerging technologies more equitable, accessible, and accountable. At the grassroots level, we empower individuals particularly women, marginalized communities, and human rights defenders with the tools and knowledge to navigate the Internet safely and assert their rights online.

Contact information:
info@digitalrightsfoundation.pk
www.digitalrightsfoundation.pk

Gender-sensitive, confidential & accessible helpline:
0800-39393
helpdesk@digitalrightsfoundation.pk

Our gender-sensitive, confidential, and accessible Digital Security Helpline aims to provide callers with a safe space where they can easily share their problems regarding technology-facilitated gender based violence and online violence. The Helpline can be contacted through phone, social media and emails 7 days a week from 9AM to 5PM (GMT+5).

This report has been compiled by: Hyra Basit, Ayesha Sarwar, Anmol Sajjad, Aneeqa Shahid
Reviewed and Edited by: Nighat Dad, Seerat Khan
Design and Layout by: Ahsan Zahid, Talha Umar
Cover page and illustrations by: Bushra Saleem

Table of Contents

A Note from DRF’s Executive Director 01

Gendered Targets, Digital Frontlines: The Helpline's Evolving Response 03

- Our Support Services 05

Year in Review - 2024 09

Age-Specific Data Trends 13

Spotlight #1 14

Access to Justice: Local & Global Reach 18

Spotlight #2 21

Gender Distribution 24

- Relation Between the Reporter and the Victim 25
- Who Are the Harassers? 26
- Relation Between the Victim and Harasser 26

A Lifeline for High-Risk & Vulnerable Groups 27

Spotlight #3 30

Tracking Digital Threats: Platform-Specific Trends and Advocacy Efforts 33

Gendered Patterns in Digital Threats: Key Trends and Insights 35

Content Takedown and Escalation Resolutions 40

Making a Difference: The Helpline's Impact 42

- Impact Survey and Analysis 44

Recommendations for Social Media Platforms 48

Recommendations for Policymakers 52

Recommendations for Law Enforcement Authorities 54

Appendix 1 57

A Note from DRF's Executive Director

As digital and civic spaces across South Asia shrink under the weight of increasing digital oppression of states and platforms, the work of the Digital Rights Foundation (DRF) has never been more urgent. Powerful actors are weaponizing disinformation to justify crackdowns on free expression, censor independent journalism, and silence dissent. Meanwhile, online spaces are becoming more hostile, especially for women, youth, and marginalized communities, due to the rise of AI-generated content, non-consensual intimate imagery (NCII), and gendered disinformation. The very platforms enabling these harms are retreating from accountability, instead devising ways that further marginalize vulnerable individuals. These are the very people our Digital Security Helpline has supported for the past eight years.

This past year, our Helpline has operated under immense pressure as the political climate continues to erode digital freedoms. The same power structures that marginalize vulnerable voices online are now attempting to stifle the very mechanisms designed to protect them. And yet, despite these threats, we remain undeterred. The Helpline stands strong, and we are preparing to expand it. Our regional footprint is growing, and our impact now resonates far beyond Pakistan, offering insights into patterns of technology-facilitated gender-based violence (TFGBV) across South Asia.

The Helpline has become the most consistent and reliable source of data on online safety and TFGBV in the region. Year after year, this data not only informs national policy conversations, but also contributes to global research on digital harms and online safety frameworks.

Over the course of 8 years however, the Helpline has expanded its scope and kept aligning itself with the needs of the people it aims to help. The transition from the Cyber Harassment Helpline to the Digital Security Helpline and Emerging Threat Lab also stems from the same purpose; as we expand the Helpline to cater to the current needs of the time, we realize that the Helpline essentially caters to much more than just TFGBV, and to a niche group of people. To reflect the very specific and specialized service we provide, we have updated our title to Digital Security Helpline, as we include an Emerging Threat Lab to our scope of work as well to address most sophisticated digital attacks against civil society organizations (CSOs), human rights defenders (HRDs) and journalists.

None of this would be possible without the dedicated human infrastructure behind the Helpline. Our digital security experts, legal team, and, most critically, our incident response analysts, who are often the first point of contact for those in distress, are the heartbeat of this work. In a time where AI and automation are hailed as the future, it's important to remember that trust, safety, and digital security are deeply contextual. Cultural nuance, emotional intelligence, and lived experience cannot be programmed. Tech companies and state actors must recognize the limits of automation—this is not a space for cost-cutting at the expense of human safety.

As we look ahead, DRF reaffirms its commitment to defending digital rights, ensuring online safety, and expanding our regional impact led by people, grounded in care, and backed by evidence. The Helpline will endure. Because our communities deserve safe, inclusive, and free digital spaces.

Nighat Dad

Nighat Dad,
Executive Director
Digital Rights Foundation

Gendered Targets, Digital Frontlines: The Helpline's Evolving Response

Pakistan already ranks as one of the most dangerous countries in the world for women, and an increase in the mobile broadband penetration in Pakistan only brings with it the threat of gender-based violence extending beyond physical spaces into the digital realm, and vice versa. While broadband and mobile broadband penetration[1] in the country reached 58.6% and 57% respectively, the gender gap in smartphone ownership[2] is 49%, and the gender gap in internet adoption stands at 38%. With only 33% of the women in the country having adopted regular internet usage, and 23% of female mobile internet users having to use someone else's mobile phone to access the internet, it is only expected that the lack of knowledge of the ecosystem means that a majority of the women would not know how to protect themselves from being the target of technology-facilitated gender based violence (TFGBV).

The increasing accessibility of technology has also led to the evolution of TFGBV, fueled by deep-rooted patriarchal and misogynistic norms. The elections in early 2024 provided a stark example of this trend, as deepfake content was widely used to target women journalists and politicians. In the course of 2024, we witnessed that gender minorities face an even greater risk, exacerbated by the anonymity and lack of accountability in digital spaces.

In a society where a woman's reputation is closely tied to family honor, access to the internet is often perceived as a threat rather than a tool for empowerment. Women and girls seeking digital connectivity face not only technological and financial barriers but also social resistance that restricts their ability to use the internet freely. Many remain unaware of their legal rights and the protections available to them when facing digital threats.

At the same time, Pakistan has also been facing increasing religious intolerance,[3] with the use of false online blasphemy allegations against religious minorities, particularly to settle personal scores. Here too, the line between online and offline harms are blurred; weak legislation, drafted without consideration for the protection and rights of religious minorities, and the complicity of law enforcement[4] often means that hate speech and

[1] Pakistan Telecommunication Authority. 2025. "Overview." PTA. https://www.pta.gov.pk/category/telecom-indicators.

[2] Jeffrie, Nadia. 2024. "The Mobile Gender Gap Report 2024." GSMA. https://www.gsma.com/r/wp-content/uploads/2024/05/The-Mobile-Gender-Gap-Report-2024.pdf.

[3] Human Rights Commission of Pakistan. n.d. "HRCP alarmed by surge in blasphemy cases against Shia community." HRCP. https://hrcp-web.org/hrcpweb/hrcp-alarmed-by-surge-in-blasphemy-cases-against-shia-community/.

[4] Ali, Imtiaz, and Ahmed B. Arisar. 2024. "Inquiry ordered into Umerkot blasphemy suspect's 'extrajudicial killing.'" Dawn. https://www.dawn.com/news/1860164.

allegations against members from religious minority communities will lead to arrest or mob violence. In a research[5] on the online experiences of religious minorities in Pakistan conducted by DRF, 61% of respondents said that they either felt unsafe or were on the fence about their comfort with expressing their opinions online. Online abuse, ranging from bullying to threats resulting in offline consequences, was reported by 55% of 83 respondents.

Moreover, minority groups often face online threats on the basis of their multiple identities; one example of the intersectional dangers that have emerged online has been the (direct or indirect) blasphemy allegations leveled against transgender folks, and the community as a whole. According to a case study by DRF, the hate speech and gendered disinformation campaign against the community resulted in the loss of employment opportunities, legal protections, severe mental health distress, in addition to online hate, slurs, threats, and dehumanizing speech. [6]

Similarly, journalists already face heightened vulnerability in online spaces, with incidents of censorship, threats, doxing, etc. According to the World Press Freedom Index, Pakistan ranks 152 out of 180 countries, dropping two places in the index in 2024.[7] Additionally, when it comes to intersectional identities, women journalists face greater consequences as a result of the hostile online environment against them. They also face gendered disinformation, sexualized threats and image-based abuse, now including AI (artificial intelligence) generated images. [8]

Recognizing the urgent need for intervention, DRF has conducted extensive research on online harassment. A study surveying women in media and information sectors found that 55% had faced online abuse, yet only 14.2% sought assistance.[9] Another report highlighted that 70% of women feared the misuse of their images online, while 40% reported stalking and harassment on digital platforms.[10]

The demand for a resource such as the Digital Security Helpline became evident through the organization's Hamara Internet project, where young women frequently sought

[5] Digital Rights Foundation. 2021. "RELIGIOUS MINORITIES IN ONLINE SPACES." Digital Rights Foundation. https://digitalrightsfoundation.pk/wp-content/uploads/2021/05/Religious-Minorities.pdf.

[6] Digital Rights Foundation. 2024. "Gendered Disinformation in South Asia Case Study - Pakistan." Digital Rights Foundation. https://digitalrightsfoundation.pk/wp-content/uploads/2024/10/DRF-Case-Study-GD-SA.pdf.

[7] Dawn.com and AFP. 2024. "Pakistan slides two places in RSF's press freedom index." Dawn. https://www.dawn.com/news/1831202.

[8] Digital Rights Foundation. 2025. "Gendered Disinformation During Elections in Pakistan." Digital Rights Foundation. https://digitalrightsfoundation.pk/wp-content/uploads/2025/03/Gendered-Disinformation-During-Elections-in-Pakistan.pdf.

[9] Digital Rights Foundation. 2019. "Fostering Open Spaces in Pakistan - Combatting Threats to Women's Activism Online." Digital Rights Foundation. https://digitalrightsfoundation.pk/wp-content/uploads/2019/04/IMS-Study-Report.pdf.

[10] Digital Rights Foundation. 2017. "Measuring Pakistani Women's Experiences of Online Violence." Digital Rights Foundation. https://digitalrightsfoundation.pk/wp-content/uploads/2017/05/Hamara-Internet-Online-Harassment-Report.pdf.

guidance on handling threats to their online presence. Additionally, the tragic case of Qandeel Baloch underscored the devastating consequences of doxxing and TFGBV, reinforcing the need for structured support mechanisms.

The passage of the Prevention of Electronic Crimes Act (PECA) in 2016, coupled with the involvement of the Federal Investigation Agency (FIA), provided a legal foundation for addressing online abuse. These developments allowed the Helpline to provide holistic support to victims of digital security incidents. Over the past eight years, the Helpline has expanded its services, strengthening its legal team and enhancing its referral network to better support victims. Although the Helpline was launched to address the growing threat of TFGBV faced by women, the scope has expanded to focus regionally on all vulnerable individuals, including journalists, human rights defenders, religious and gender minorities, and youth.

Since its inception, the Digital Security Helpline has handled **20,020** cases (*see Appendix 1*), with women consistently forming the majority of those seeking assistance. Currently, 58% of all individuals who have reached out to the Helpline are women, highlighting the urgent need for continued advocacy and systemic change to create a safer online space.

Our Support Services

We offer a range of digital security and online protection services to help individuals safeguard their online presence and respond to cyber threats.

Account & Platform Assistance

1. Remove impersonation of accounts, groups, or pages created by fake users or perpetrators.
2. Reactivate accounts, groups, or pages that were wrongfully suspended.
3. Restore hacked accounts, groups, or pages.

Digital Security Guidance

Our incident response analysts provide personalized digital security tips and tools to help protect against:

1. Device hacking or confiscation
2. Malware-infected devices
3. Phishing and social engineering tactics
4. Digital surveillance threats
5. Data breaches and data encryption attacks
6. AI-generated and manipulated images, videos, or audio used for deception

Content Removal Support

Through our Trusted Partner channels, we assist in the removal of harmful or abusive content, including:

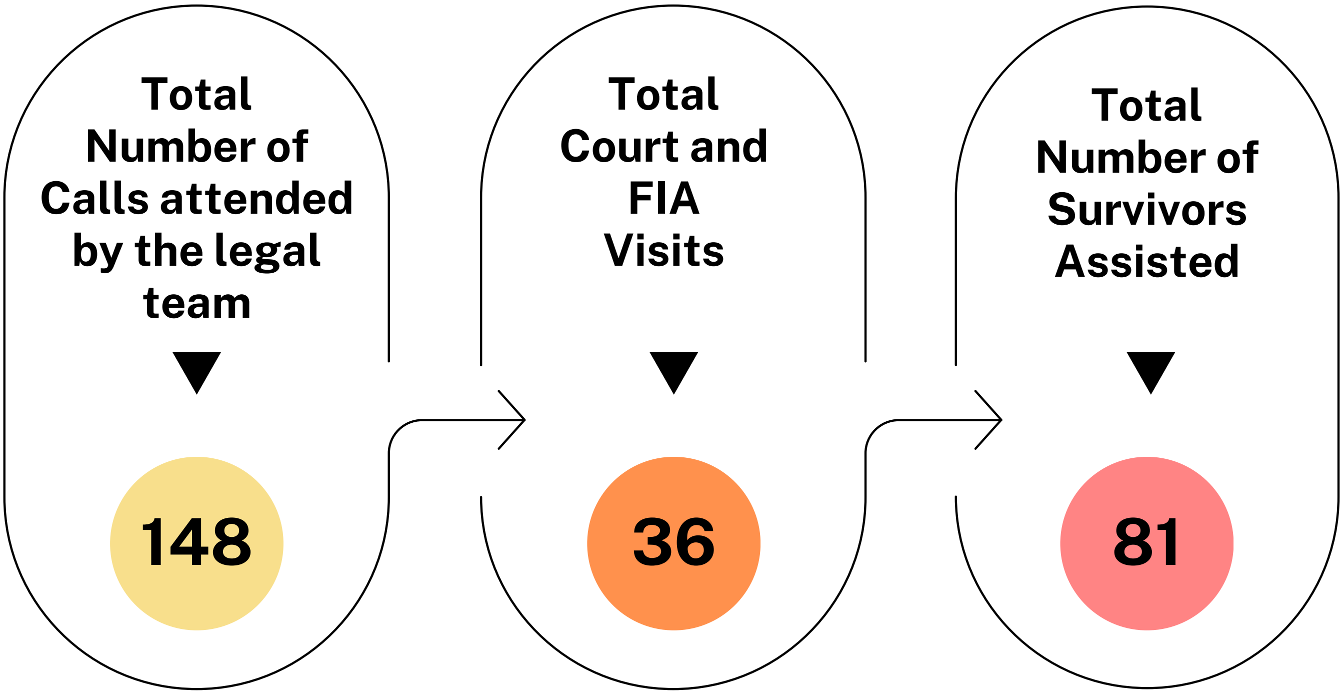
1. Online harassment & cyberbullying
2. Doxxing
3. Hate speech & incitement
4. Disinformation & defamation campaigns

5. Content related to device theft

6. Impersonation or identity theft

Expanded Legal & Counseling Support

As a digital security and threat response helpline, we continuously adapt and expand our services to meet the evolving needs of our callers. Our efforts go beyond immediate assistance—we provide long-term support through legal aid, counseling, and advocacy.



Total Number of Calls attended by the legal team ▼ 148

Total Court and FIA Visits ▼ 36

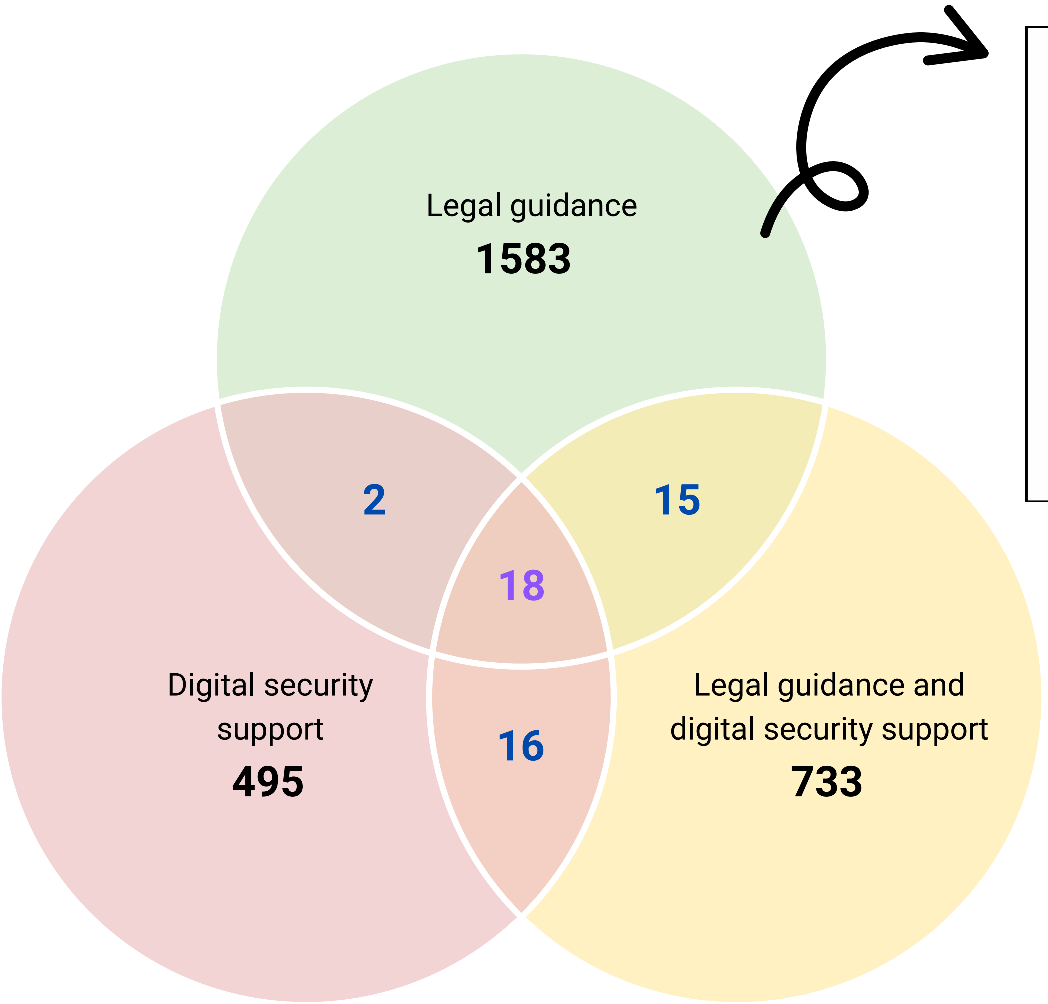
Total Number of Survivors Assisted ▼ 81

1. Our online legal directory, ‘Ab Aur Nahin’, connects individuals with pro-bono lawyers across the country, offering free legal assistance for those facing tech-facilitated gender based violence and digital threats.

2. We also provide in-person counseling and legal aid for individuals filing cybercrime complaints with FIA's cybercrime wing in Lahore, ensuring they receive guidance throughout the legal process.

Mental Health and Psycho-social Well-being

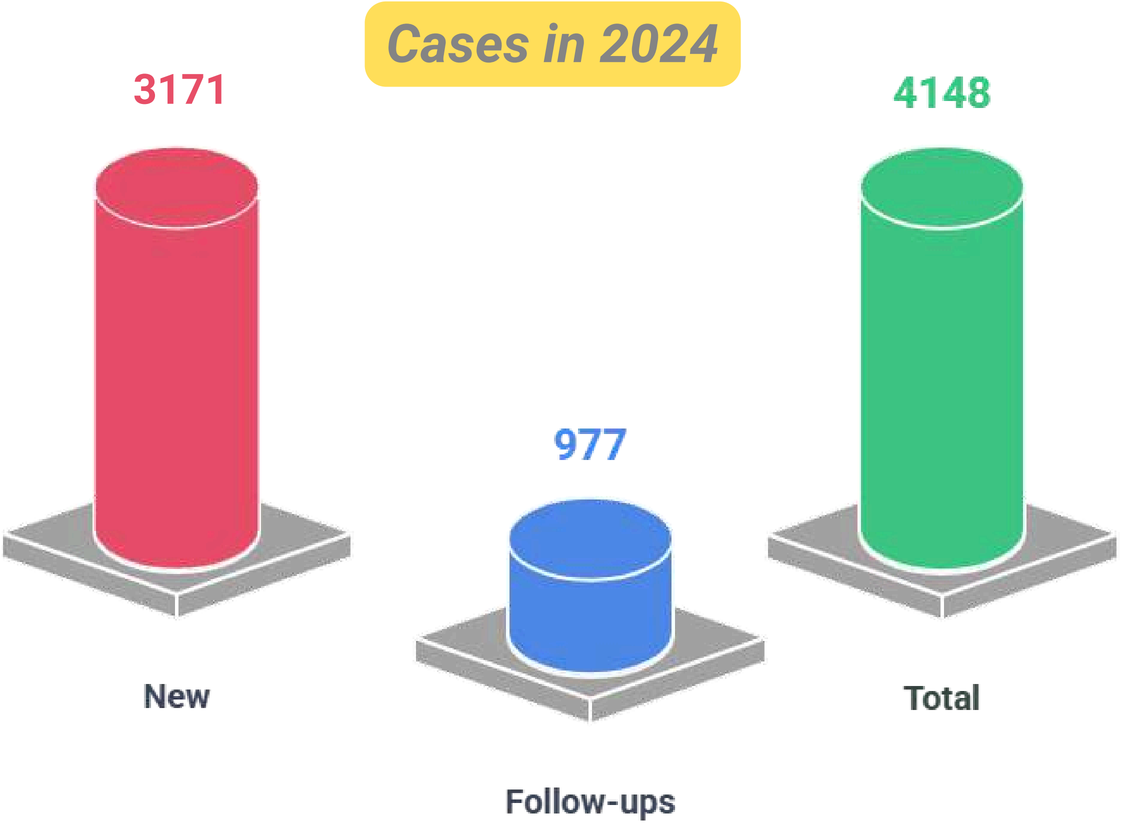
Oftentimes, the Helpline is the first and only support available to vulnerable individuals, especially women, children, and religious and gender minorities - individuals who fear being victim-blamed or face harsh repercussions based on their identity, either from their families or law enforcement. We recognize the sensitivity of digital security cases and prioritize the confidentiality and protection of our callers' information. Our strict data privacy protocols ensure that personal details remain secure and undisclosed. Furthermore, our team is trained to handle cases with discretion and professionalism, creating a safe and supportive space for individuals seeking help. Feedback received from our beneficiaries often highlights the non-judgemental, supportive and calm response received from the Helpline when seeking support.

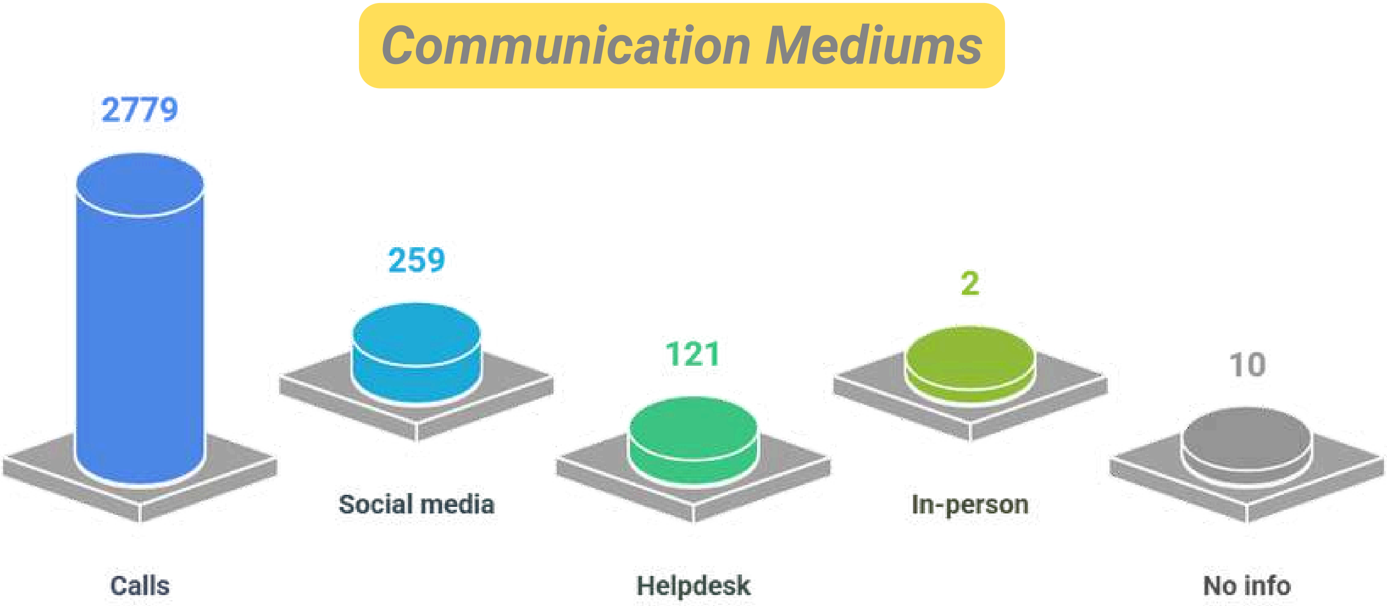


- Legal guidance: **1,583**
- Psycho-social counseling: **15**
- Digital security support: **495**
- Digital security support and psycho-social counseling: **2**
- Legal guidance and digital security support: **733**
- Legal guidance and psycho-social counseling: **16**
- All of the above: **18**

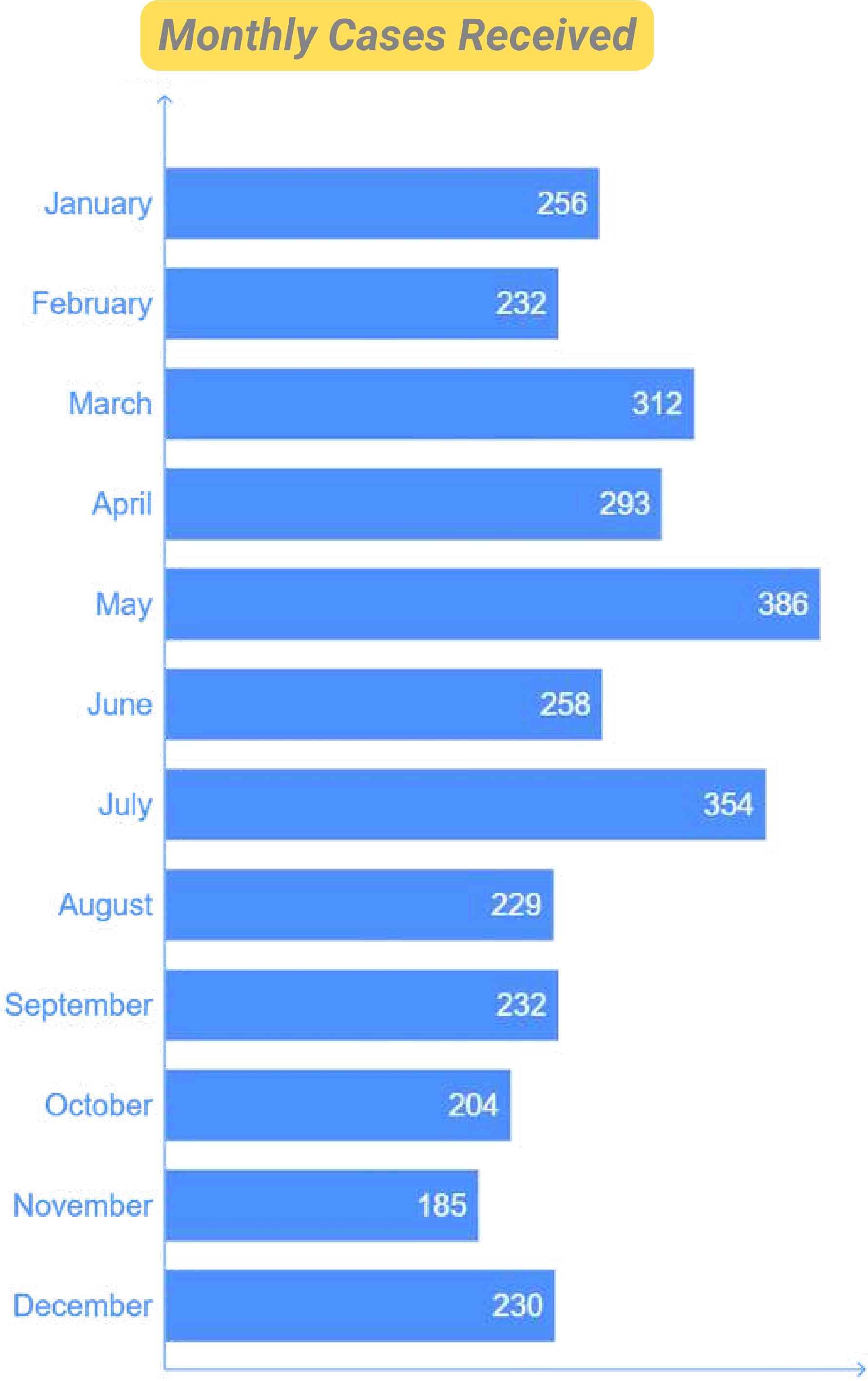
Year in Review - 2024

In 2024, the Digital Security Helpline received **3,171 new cases** through three primary channels: the Helpline phone service, the Helpdesk email, and DRF's accounts on social media platforms. The majority of incidents—**2,779 in total**—were reported via the helpline, reinforcing its role as the primary point of contact for victim-survivors seeking assistance from all over the world.





While the Helpline primarily addresses online harassment, it also considers other complaints where capacity allows, recognizing the overlap between TFGBV and other forms of violence. On average, the Helpline handled **264 new cases per month**, with **May being the busiest month of the year.**



The year started off with multiple incidents of gendered disinformation and AI generated images of women politicians and journalists, as Pakistan geared up for elections in February 2024. The use of AI to generate images of prominent women in the public sphere, especially those who were involved with the electoral process and information integrity during the election, was an attempt to humiliate and discredit the women, both in their professional and personal capacity. The normalization of emerging technology to target women in the public sphere also introduced this tool for abuse of regular women.

Further along in the year, women journalists were also targeted through the use of (false) blasphemy allegations.[11] Keeping in mind the history of blasphemy allegations in Pakistan, these accusations, that are made as a pressure tactic to censor and control the topics that journalists speak on, can result in offline harm, including mob violence and lynchings. One journalist was targeted with a coordinated online campaign to discredit and silence her, using derogatory language, gendered slurs, and death threats. In an interview with DRF, she described how this was the first time she feared for her life despite prior instances of online harassment.[12] Then again, another senior journalist was targeted on the basis of her comments regarding a blasphemy case that had occurred in the country.[13] Her X (formerly Twitter) account was hacked, in addition to a wave of coordinated attacks against her religious identity, professional and personal credibility.

Women's right to education, work, and owning mobile phones were also questioned by a seemingly religious leaning individual who produced and uploaded songs across multiple platforms.[14] The songs were directed at the 'honor' of men in the family who 'allow' women and girls in their family to avail these opportunities. The religious connotation in the videos could be one reason why the videos garnered views and approvals in the thousands, but our more immediate concern at the Helpline was flagging to platforms the dangers of such videos in Pakistan's context, and grappling with their rejections or slow response rates. YouTube in particular put up strong resistance to removing these videos that put women's physical safety and their right to education among other things, at great risk.

Furthermore, the PECA law, that addresses cybercrimes, went through much debate throughout the year. Towards the end of the year, it was eventually amended to include sections that primarily address 'fake news' and misinformation, but was heavily criticized and protested against by the journalists, media bodies, and digital rights activists.[15] However, even before the proposed amendments, policymakers had already created an environment of confusion for the targets of TFGBV earlier in the year, and for law enforcement, when they announced the formation of a new body that would investigate

[11] Imran, Sara. 2025. "› Senior journalist Munizae Jahangir target of hate speech for discussing perpetrators behind fake blasphemy allegations." Digital Rights Foundation. https://digitalrightsfoundation.pk/senior-journalist-munizae-jahangir-target-of-hate-speech-for-discussing-perpetrators-behind-fake-blasphemy-allegations/.

[12] Digital Rights Foundation. 2024. "Gendered Online Hate in Pakistan - Right Wing Religious Campaigns Against Women Journalists." Digital Rights Foundation. https://digitalrightsfoundation.pk/wp-content/uploads/2024/12/Gendered-Online-Hate-in-Pakistan-Right-Wing-Religious-Campaigns-Against-Women-Journalists.pdf.

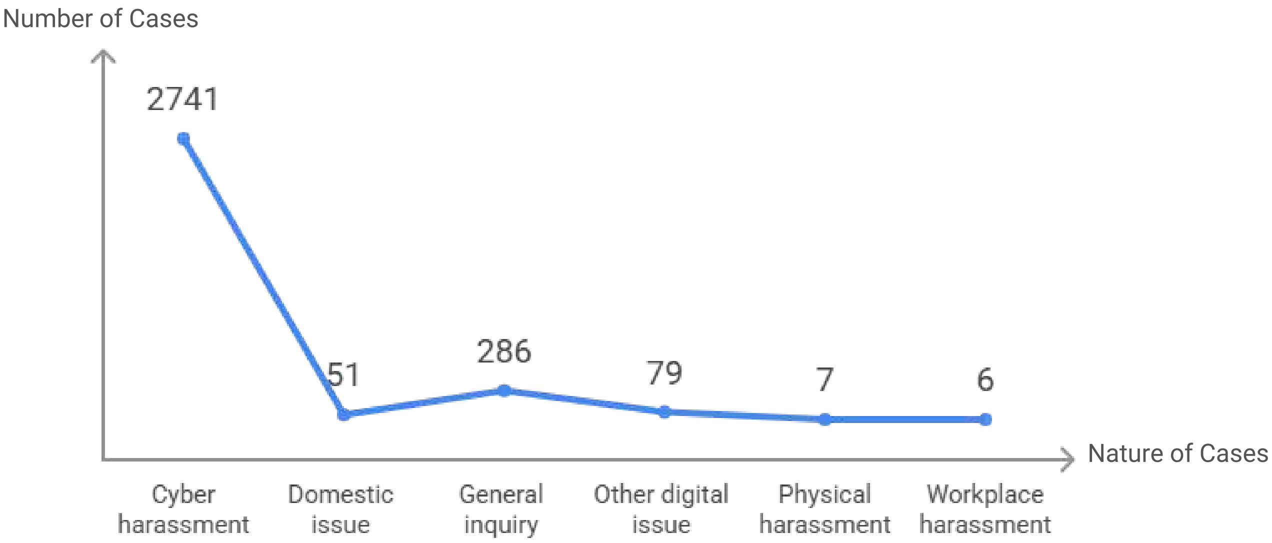
[13] "Pakistan: Benazir Shah Endures Coordinated Online Harassment and Hacking - Women Press Freedom Calls for Stricter Regulations — Coalition For Women in Journalism." 2024. Coalition For Women in Journalism. https://www.womeninjournalism.org/threats-all/pakistan-benazir-shah-endures-coordinated-online-harassment-and-hacking-women-press-freedom-calls-for-stricter-regulations

[14] Chishti, Hasan I. 2024. "Apni Dhi Schoolo Hata Le | Othy Dance Kardi Payi Ae | Kalam Hasan Iqbal Chishti." YouTube. https://www.youtube.com/watch?v=SjADMZPAPoc.

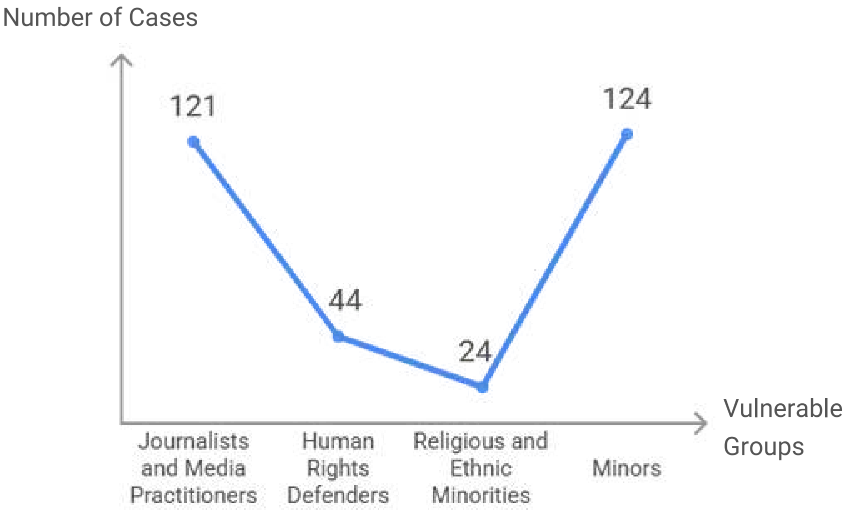
[15] The Express Tribune. 2025. "Senate approves PECA amendment bill amid journalists' walkout." The Express Tribune.https://tribune.com.pk/story/2525031/senate-approves-peca-amendment-bill-amid-journalists-walkout.

cybercrimes, and the dismantling of the cybercrime wing of the FIA.[16] The haphazard manner in which the announcement was made, without having formalized any rules, left citizens in the limbo when these types of cases require immediate resolution. A few months later, the announcement was taken back suddenly and without explanation.[17]

Types of Cases Received



Cases Involving Vulnerable Groups



You helped me and made me comfortable. Talking to you took all my fear and I am confident that this case would meet success soon.

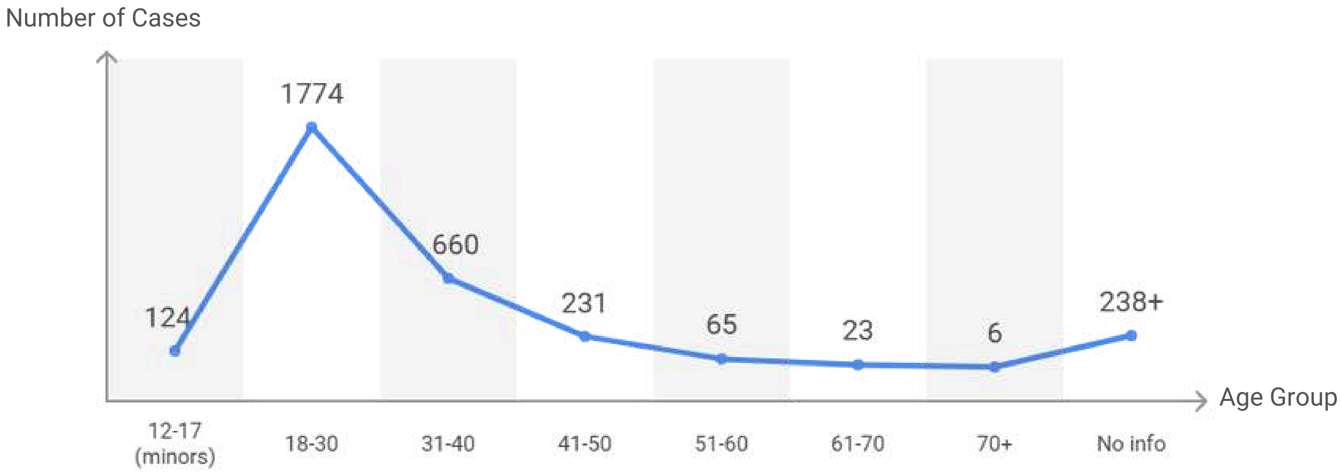
[16] Momand, Abdullah, Abbas Nasir, and Ahmed B. Mehboob. 2024. “Govt notifies new cybercrime investigation agency to tackle Peca offences.” Dawn. https://www.dawn.com/news/1831222.

[17] Ali, Kalbe. 2024. “Govt disbands NCCIA, revives FIA wing - Pakistan - DAWN.COM.” Dawn. https://www.dawn.com/news/1878233.

Age-Specific Data Trends

This year, **the Helpline observed a remarkable 51% jump in the number of children and youth under the age of 18.** Analysis of complainant demographics reveals that women make up the majority of complainants in the **18-30 age group** (over **62%** of cases). Notably, in age groups above 30, a higher number of men filed complaints compared to women. This trend may suggest that younger women experience online harassment at higher rates, or it could indicate that they feel more confident with coming forward to report such incidents. However, without further data, the precise reason for this disparity remains inconclusive.

Cases received by Age Group



> *I have nothing to add. My experience with the Helpline was smooth, prompt, well explained, methodical and there was a lot of regard and sympathy for my situation.*

Spotlight #1

Threat incidents faced by children are prioritized by the Helpline, and we have seen a considerable increase in the number of youth who reached out to us this year. When their already vulnerable state is heightened further by the inability to travel long distances, financial restrictions, and investigation delays, the Helpline tries its best to intervene in any way possible, and present alternate solutions as well.

Case Description:

Photos of two sisters, aged 14 and 17 years, were being posted on TikTok. The perpetrator reached out to their aunt through the fake profiles and demanded to get in touch with the girls. In the first phase, the family decided to get the accounts taken down instead of pursuing legal action to keep the peace in the family. The accounts were removed with the Helpline's intervention. Through the one account that was left active, he reached out again, sharing a manipulated intimate image of the 17 year old girl. The father reached out to the Helpline again, this time wanting to pursue legal action. In response, the Helpline used their established network with law enforcement (All Pakistan Child Pornography Incharge) to facilitate the case. We spoke with the girls' father to hear his account of the events.

Spotlight #1

Transcription:

I tried calling Cyber Crime Rawalpindi regularly for two days, but no one picked up. After that, I dialed another helpline, and they gave me your helpline number. I didn't know which city you were located in and didn't have any information. I spoke to you on the phone, and you reassured me and got the account taken down. The IDs that were taken down by you is the only progress in this case otherwise, no action has been taken so far. I got complete cooperation and support from you. It's because of you those TikTok accounts got taken down.

I tried calling Cyber Crime in Rawalpindi, but they never picked up. Thank God, I'm very relieved that you helped me get in touch with them, and some of the issues are getting resolved. It still hasn't really started getting sorted out, but it is in progress.

At that time, I had made the decision to end my life, but then I thought about my family and couldn't find the courage to go through with it. Otherwise, I would have done it. My family supported me, but I was feeling hopeless. I mean, what can you do when life challenges you like this? Some days are good, and some days are bad.

No one apart from the immediate family or a few of my friends know about this issue. I had thoughts like my daughter is still young and I need to think about her future marriage prospects so only a few people know whom we trust. My family is still with me but at this point they are saying that the accounts have been taken down so I should let this matter go. I have stopped telling

Spotlight #1

my family whenever I am visiting the FIA Office now and what steps I am taking. I go to Rawalpindi from work and return home in the evening. My belief is that whatever happened to me has already happened, at least no one else should go through the same thing.

My daughter is 17 years old. I have tried my best that her life either education or extra curricular activities are not affected by this incident. We haven't blamed her or beat her after this incident happened, we are not like that. In the initial weeks following the incident, my daughter seemed very frightened. An incident like this is a stain on a girl's character, once happened you can't really wash it off at any stage of life even after 5 or 10 years. Things like these always come to light and it causes a lot of difficulties in your life.

At the FIA (law enforcement office), they listen and talk calmly any time I visit the office. But as far as my case is concerned, they keep saying that we'll send an application in court to get information on these accounts from TikTok. After getting approval from TikTok through court, then the issue will be resolved to some extent. From that day to this day, it's the same response that I get. I am from a lower-middle class so every time I visit, it costs me around Rupees 5000. I also have to think about my work. I can't afford it anymore, to be honest. It's been 2 months now and they keep saying the same thing, to come back again after 10 to 15 days.

Spotlight #1

I have made a decision that the next time I visit will be the last one. If this matter gets resolved that's good otherwise, I'll let it go. It's the only solution for a poor person. What more can we do? I can't pay money to expedite the case. The case is still standing on the same point it was started. The pictures that were taken down were by your intervention is the only resolution that has happened other than that there has been no progress.

Nothing can be done in Pakistan. Like I said, you either need a bribe or a recommendation (verbatim: sifarish*) from somewhere. I don't have either, and even if I did, I wouldn't pay a bribe for something like this. Allah is my helper, a poor person can only do this. I say this because I have been visiting FIA for two months, and every person there has the same story. Some people have been stuck for one and a half or even two years, and they are told the same thing and that is to come back again after 10-15 days. I know this because I visit regularly.*

Access to Justice:
Local & Global Reach

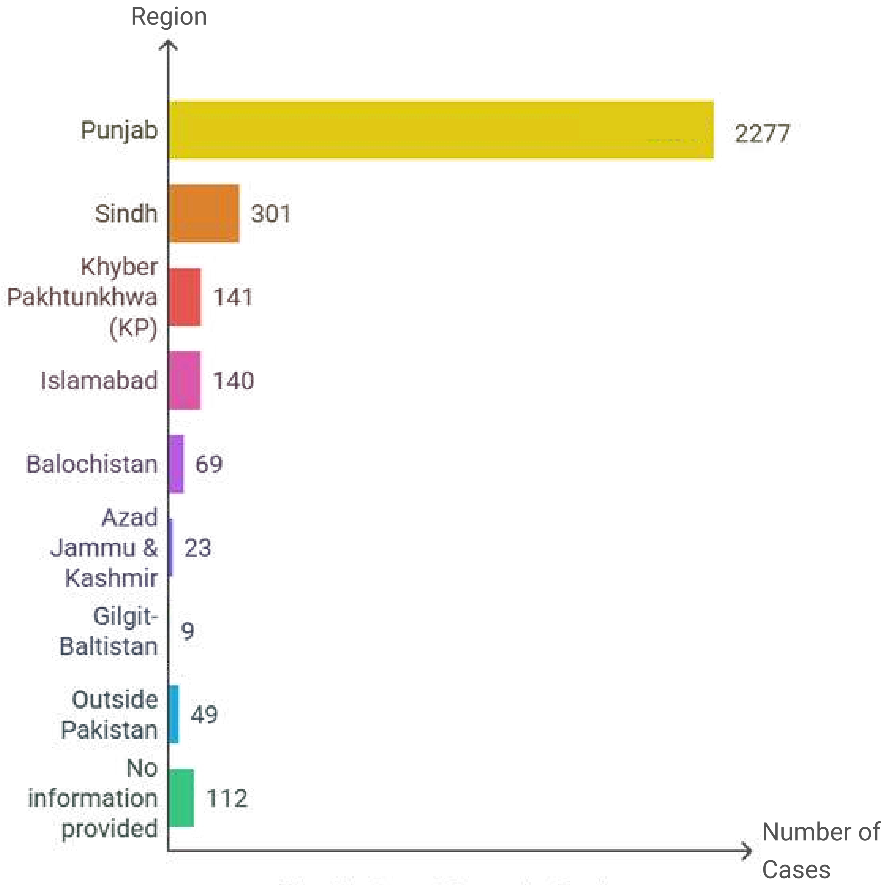
To provide targeted support and policy advocacy, the Helpline collects data on the city and region of complainants. This information helps identify gaps in access to justice and strengthens efforts to improve legal protections and digital safety for vulnerable groups.

The Digital Security Helpline is more than just a resource for the people of Pakistan; **in 2024, the Helpline catered to requests from 25 countries.** Over the years, it has established itself as a lifeline for women and vulnerable individuals from all over the world, and has provided crucial digital security support for threat incidents. Despite our global presence, the majority of cases received still happen to be from Pakistan, but we use our dataset and insights from our practice over the years, to inform our regional and global advocacy.

Afghanistan	2
Nigeria	1
Algeria	3
Kashmir	21
Bangladesh	6
Denmark	1
UAE	3
Central Africa	1
Finland	1
France	1
India	3
Iraq	1
Ireland	1
Malaysia	1
USA	5
Philippines	1
Saudi Arabia	2
Spain	1
Sweden	1
Turkey	1
South Africa	1
UK	5
Vietnam	1
Unknown	3

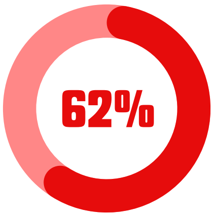
The following is a provincial and territorial distribution of the cases received by the Helpline within Pakistan in 2024:

Cases Received by Province\Territory



As in previous years, **Punjab continues to report the highest number of cases**, reflecting both its larger population and greater awareness of the Helpline. A notable increase in cases from Sindh and Balochistan compared to previous years suggests either greater outreach efforts or rising digital threats in these regions. However, Gilgit-Baltistan and Kashmir remain underrepresented, which could indicate lower digital literacy, a lack of reporting awareness, or inadequate access to legal support.

- **Out of the 2,741 cyber harassment cases, 1,703 (62%) were referred to the FIA for legal intervention.**



- **Of these, only 619 cases (36%) originated from cities where an FIA cybercrime wing is operational, requiring many complainants to travel to another city to file a formal complaint.**

This data indicates significant accessibility challenges, particularly for those in remote areas or smaller cities. Survivors often face logistical, financial, and cultural barriers when attempting to pursue legal action, discouraging many from seeking justice. Women, in particular, face additional constraints, as they are often dependent on male family members for mobility, financial support, and permission to engage with law enforcement.

With a significant proportion of complainants residing in areas without an FIA cybercrime wing, many victims lack timely and accessible legal recourse. The consistent rise in cyber harassment cases highlights the urgent need for stronger digital protections, including policy reforms, greater enforcement of cybercrime laws, and increased investment in awareness campaigns. Addressing these systemic barriers is crucial for ensuring that all individuals, particularly women and marginalized groups, have equal access to justice and protection in digital spaces.

Cases Received by City

940	🟥	City without FIA office
8	🟩	Abbottabad
152	🟥	Faisalabad
9	🟥	Gilgit
101	🟪	Gujranwala
2	🟥	Gwadar
33		Hyderabad
140		Islamabad
224		Karachi
900		Lahore
129		Multan
55		Peshawar
56		Quetta
167		Rawalpindi
11		Sukkur
9		DI Khan
65		Out of jurisdiction
120	🟥	No info

Spotlight #2

Each year, we receive multiple incidents of cross-border intimidation and harassment. Even though PECA states that the law applies to all Pakistani citizens anywhere in the world, the implementation of this provision leaves much to be desired. TFGBV survivors whose perpetrators leave the country are often left waiting in dread without immediate solutions because of the lack of collaboration between law enforcement agencies across borders (*see Recommendations chapter*). Many times, women bear the brunt of this burden, as they are blamed for their situation, their character is questioned, and restrictions are placed on their device ownership and movement.

Case Description:

The complainant, a 21-year-old woman from Bahawalpur, was in a relationship with her cousin. However, when her family rejected his marriage proposal, he retaliated by sharing her intimate pictures and videos with her family members, including her parents, uncle, and cousins. The family pursued legal action and filed a case with the FIA in Lahore. The FIA instructed them to call the harasser to Lahore to facilitate his arrest. However, he is now planning to leave the country for Dubai.

Spotlight #2

Transcription:

At first, I didn’t realize what was happening. Slowly, I started noticing the threats. He would message me every week, sometimes multiple times, demanding that I talk to him—otherwise, he would tell my family everything.

For a year, I tried to handle it alone. But when things spiraled out of control, I told my aunt. We traveled to Lahore to report the case, only to be told we had to go to the FIA office in Multan instead. There, the FIA officers asked us to lure him into a meeting so they could arrest him. But by then, he had already left the country. That’s when fear truly set in. I was terrified that my videos would be leaked. Desperate for help, I searched YouTube and found your Helpline. I spoke with Zainab (incident analyst at the Helpline), who guided me and gave me hope. My family, however, blamed me. They insisted we shouldn't go to cybercrime authorities, fearing dishonor. For months, they pleaded with his family, asking them to take action, but they refused. Left with no other option, we filed a complaint.

This experience changed my life. I had to drop out of school. I wasn’t allowed to leave the house, and my phone was taken away. My family lost trust in me. Before, they believed in me, but now, that trust was shattered. The Helpline became my only support. They explained everything, guided me through each step, and even connected me with an FIA officer in Multan. Their encouragement helped me regain hope. The FIA eventually arrested him before he could flee to Saudi Arabia. They seized his phone and deleted my data.

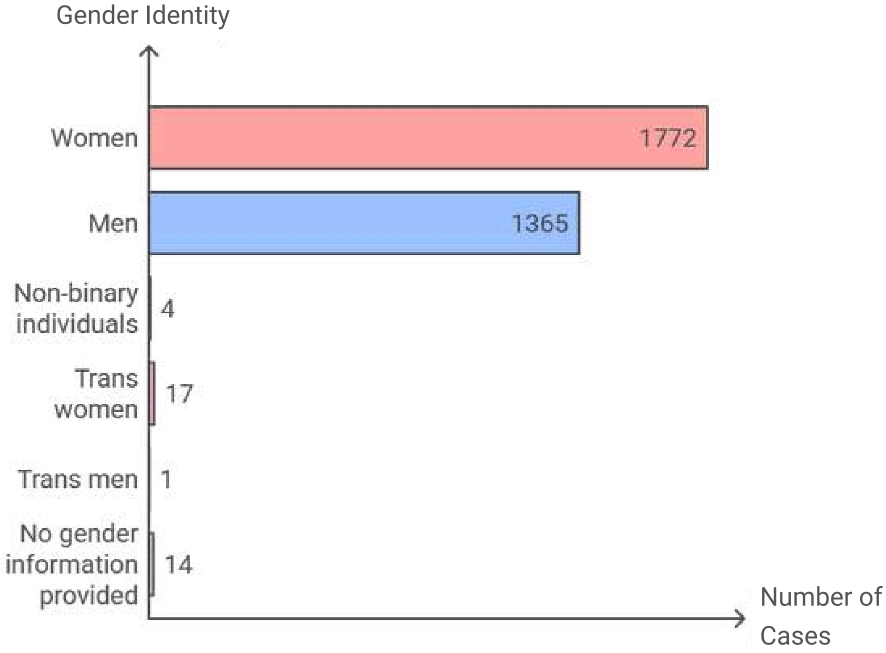
Spotlight #2

But the nightmare wasn't over. He had another phone, left in Dubai, still containing my videos. That phone hasn't been recovered, and I still live in fear. If online case filing had been an option, things would have been easier. We wouldn't have had to travel back and forth, struggling because we had no connections within the FIA. When we first went to Lahore, no one listened. But with the Helpline's support, the officer in Multan took immediate action. Even though the FIA initially followed up frequently, their response slowed over time. If they had acted sooner, they could have arrested him before he even planned to leave the country. Despite everything, I'm grateful that justice was served—but the fear lingers.

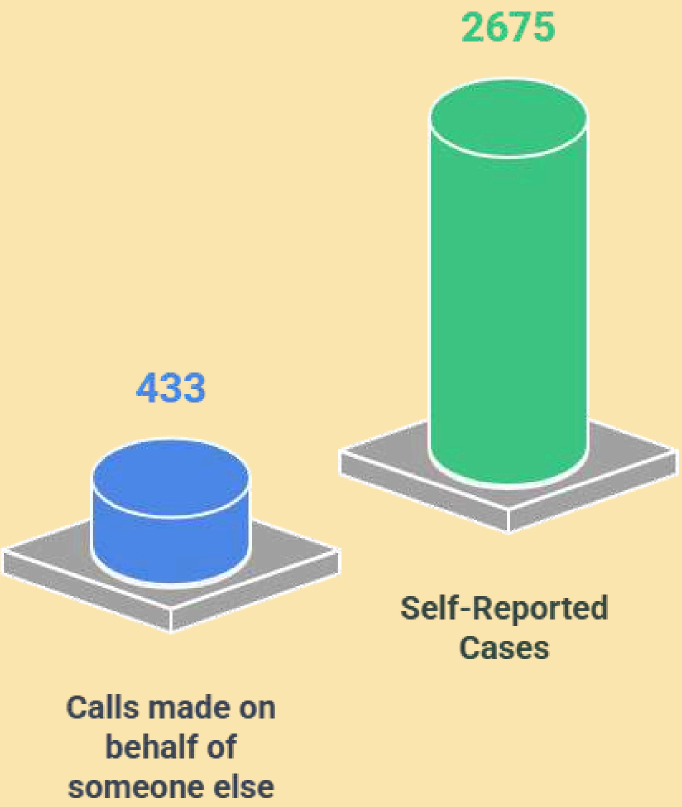
Gender Distribution

The Helpline remains a critical resource for women and gender minorities, offering a safe space to report TFGBV without fear of judgment. The latest data highlights persistent gender disparities in online harassment, the challenges of reporting, and the urgent need for more accessible support mechanisms.

Breakdown of Cases by Gender



The data confirms that **women continue to be the primary targets of online harassment**, accounting for the majority of reports. However, men also report significant instances of online abuse, highlighting the need for broad-based digital safety interventions. The low number of reports from transgender individuals suggests potential barriers to seeking help, including fear of discrimination, lack of trust in reporting mechanisms, and systemic legal challenges.



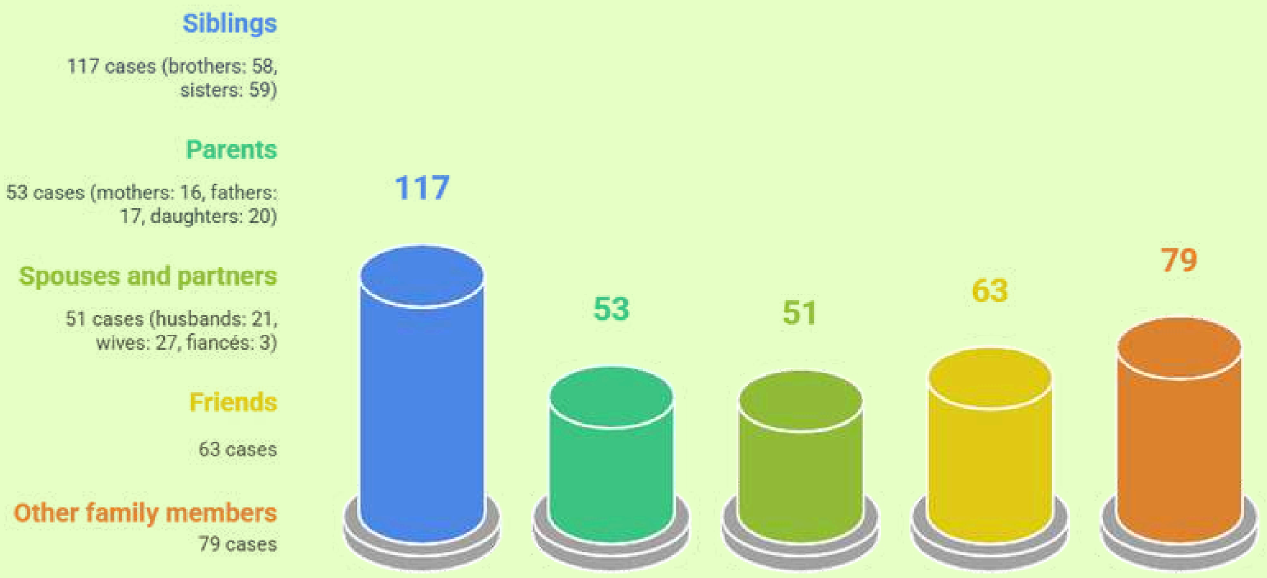
In Pakistan's conservative social landscape, being a victim of online harassment carries significant stigma, often leaving individuals, particularly women, isolated and without support. Cultural and familial restrictions make it difficult for women to confide in relatives or seek help, reinforcing a cycle of silence and vulnerability. The GSMA Gender Gap report highlights that family disapproval remains a major barrier to women's access to mobile phones, further limiting their ability to seek assistance for digital threats.[18]

Many women who reach out to the Helpline express an inability to share their experiences with family, fearing blame, judgment, or even punitive consequences. This lack of a safe support system is precisely why the Helpline exists: to provide a confidential, judgment-free space where survivors can regain control, access resources, and take steps toward justice without fear of further victimization.

The high percentage of self-reported cases (86%) suggests that most victims prefer to seek support directly, rather than relying on family or friends to intervene. However, 433 cases were reported by third parties, indicating that some survivors, particularly women, may feel unsafe or unable to come forward themselves.

Relation Between the Reporter and the Victim

While the majority of complaints were self-reported, those reported on behalf of someone else were most frequently from:



This data suggests that when victims do not feel comfortable reporting themselves, they are most likely to turn to close family members, particularly siblings and parents.

[18] Jeffrie, Nadia. 2024. "The Mobile Gender Gap Report 2024." GSMA. https://www.gsma.com/r/wp-content/uploads/2024/05/The-Mobile-Gender-Gap-Report-2024.pdf.

Who Are the Harassers?

- Majority of reported harassers were male (673 cases), reinforcing the well-documented trend that women are disproportionately targeted by male perpetrators.
- 103 cases involved unknown perpetrators, reflecting the challenge of identifying online harassers due to anonymity in digital spaces.

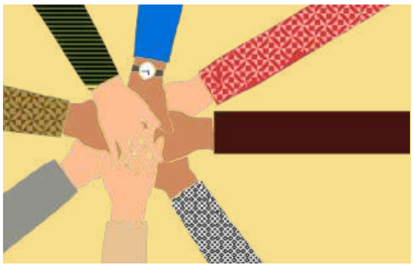
Relation Between the Victim and Harasser

- Ex-husbands and ex-partners accounted for 218 cases, with 208 involving male ex-husbands/partners harassing women. This is a significant pattern, demonstrating that online harassment is frequently linked to intimate partner violence, particularly following breakups and divorces.
- Family members were reported as harassers in 48 cases, indicating internal family dynamics contributing to online abuse, such as honor-related harassment or controlling behavior.
- Strangers and unknown individuals made up a large proportion of reported harassers (157 cases), emphasizing the risks of random, opportunistic cyber harassment based on anonymity.
- Consumers/clients harassing individuals accounted for 63 cases, which is particularly relevant for women in the workforce, including freelancers and online business owners, who often face gendered abuse in professional settings.

> *I felt safe after talking to you. I was ready to comply with his every demand but after our conversation, I am much more confident in the legal procedure and willing to take action.*

By addressing these structural and social barriers, the Helpline continues to serve as a crucial support system, ensuring that survivors of TFGBV, regardless of gender identity, have access to justice and protection.

A Lifeline for High-Risk & Vulnerable Groups



As digital spaces increasingly become extensions of real-world socio-political tensions, certain communities and professions are disproportionately vulnerable to online threats, cyber harassment, and digital security breaches. These individuals often lack institutional protection, making the role of the Digital Security Helpline even more critical as a specialized incident response service.

The past year saw sustained, coordinated digital hate campaigns, particularly targeting transgender individuals, journalists, and activists. The trans community continued to face severe online harassment, including threats of physical violence, legal intimidation, and gendered disinformation campaigns, directly endangering their safety and well-being. In response, the Helpline intensified its engagement with social media platforms, advocating for stronger enforcement against hate speech and abuse.

Journalists and media practitioners also remained prime targets of cyber harassment, facing misogynistic abuse, doxxing, and organized smear campaigns. Women journalists were particularly impacted, often enduring explicit gendered image based abuse that jeopardized their professional standing and personal safety. The use of threats and disinformation grounded in religious sentiments has become a common and powerful tool to silence and endanger journalists and activists alike. AI generated images, audio, texts, and videos, which are hard for laypeople to differentiate from genuine content, also puts the journalists' and HRDs' safety in jeopardy. We have also seen emerging patterns of the families of these vulnerable individuals being targeted online to pressurize the same individuals, including instances of manipulated images of wives and daughters of public figures. The Helpline provided tailored digital security assistance, advising journalists on threat mitigation, secure communication, and crisis response strategies.

Beyond individuals, government figures, lawyers, and civil society organizations also encountered cyber threats, particularly in politically charged online environments. The Helpline received multiple cases of targeted hacking attempts, phishing attacks, and digital surveillance concerns affecting these professions.

Breakdown of Cases Involving High-Risk and Vulnerable Groups

- Journalists (113)
  - 65 Female
  - 48 Male
- Activists (45)
  - 27 Female
  - 14 Male
  - 4 Trans Female
- Artists (4)
  - 3 Male
  - 1 Female
- Civil Society Representatives (4)
  - 3 Female
  - 1 Male
- Government Figures (7)
  - 5 Female
  - 2 Male
- Government Organizations (1)
  - 1
- Lawyers (10)
  - 4 Female
  - 6 Male
- Media Practitioners (8)
  - 3 Female
  - 5 Male
- Scholars (2)
  - 1 Female
  - 1 Male
- Other Professions (1)
  - 1 Male

Additional Vulnerable Groups

- Religious Minorities (14)
  - Female: 7
  - Male: 7
- Ethnic Minorities (9)
  - Female: 3
  - Male: 6
- Queer Individuals (6)
  - Male: 6
- Trans Community (16)
  - Trans Women: 15
  - Trans Man: 1
- Persons with Disabilities (9)
  - Female: 2
  - Male: 7
- Minors (124)
  - Female: 69
  - Male: 55

As the Helpline pivots toward becoming a regional digital security and threat response service, our key priorities include:

01

Strengthening emergency response mechanisms for high-risk cases, particularly those involving doxxing, phishing, and cyberstalking, and malware attacks.

02

Enhancing cross-border collaboration to extend digital security assistance beyond Pakistan, making it a regional resource for individuals facing digital threats.

03

Developing proactive security training for journalists, activists, and vulnerable communities to equip them with defensive digital skills.

04

Expanding engagement with global tech platforms to advocate for stronger content moderation policies that protect marginalized groups from digital harm.

> *I was not expecting someone to be this helpful without being rude and blaming the victim. I was sceptical but I am glad I called.*

Spotlight #3

The Helpline acts as an intermediary between the marginalized communities we serve in the Global Majority and tech companies based in the Global North. What this often means is that because these companies miss or are unwilling to understand the nuances of consequences that seemingly 'minor' forms of harassment can have in certain regions, we step in to advocate for vulnerable individuals and communities. Because both state and law enforcement, and tech companies have set up their systems so that it becomes almost impossible for targets to even ask for help, let alone receive it, the Helpline's work becomes crucial to fill in that gap.

Case Description:

Case Description: The beneficiary (a journalist) and his family belong to a small, conservative area in the Sindh province of Pakistan. Photos of the beneficiary's immediate family members (wife, and two young girls) were being uploaded on Facebook with defamatory captions. The harasser used fake accounts, posting the content briefly before deleting it and deactivating the profiles, making it difficult to trace. Screenshots of these posts began circulating within their social circle, adding to their distress. Despite a year long investigation lodged with the FIA, he was unsuccessful in getting the violating content taken down. The accounts were taken down through escalation requests made using the Helpline's Trusted Partner channels.

Spotlight #3

Transcription:

We reached out to Meta multiple times for the removal of the ID and posts which usually appeared in our local language, but we got the same response from them - that the post does not violate their community guidelines. We were unable to explain to them that although the post does explicitly violate community guidelines, in our culture this type of post can become a matter of honor killing. We felt helpless. The fear of being exposed and humiliated in our society was overwhelming. Meta has developed their community guidelines according to their culture, ignoring the fact that they are running their platform worldwide and they have millions of people who are using the platform with diverse cultural backgrounds.

We also reported the issue to FIA Cyber Crime, but the process was frustrating and exhausting. We had to visit their office, which was three hours away by car, multiple times, and each time they asked for more documents and proof. They kept saying they were waiting for Facebook's response, but nothing happened. FIA even asked us to bring the affected girl, a minor, to their office, which was very difficult and could have impacted her mental health as she was unaware of the situation. Despite the local police writing to the FIA, nothing changed. The FIA couldn't trace the person because the posts were deleted and posted again at great frequency.

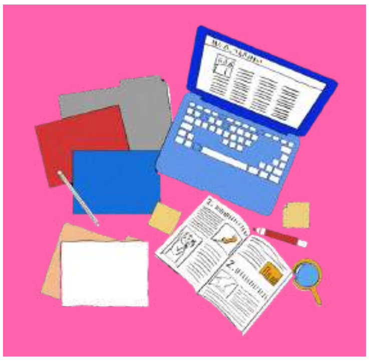
Spotlight #3

We searched online for help and found DRF. I'm glad to share that they responded immediately. A representative called me, listened to my story, and truly understood our situation. DRF helped us in ways the FIA couldn't. Their Helpline team directly contacted Meta to remove the first fake account. When the second account appeared, Facebook asked for too much information, but DRF explained our cultural context, highlighting the risk of honor killings. Finally, Facebook removed the accounts.

Although FIA couldn't track the harasser, removing the accounts sent a message that such harassment wouldn't go unchallenged. Based on my experience, I believe Facebook's guidelines should consider cultural differences, as what seems harmless in the West can be life-threatening here. The FIA's process also needs improvement. The offices should be available in every city, or cases should be handled by local police. Cyber harassment must be taken seriously, and criminals must be tracked and punished even if the post is removed.

Although the harasser wasn't caught, their accounts were taken down, which gave me hope. Now I know DRF is there for support. I tell everyone about them because they keep your identity safe and take action when no one else does. To anyone facing online harassment: don't stay silent. Help is available, you just need to reach out.

Tracking Digital Threats: Platform-Specific Trends and Advocacy Efforts

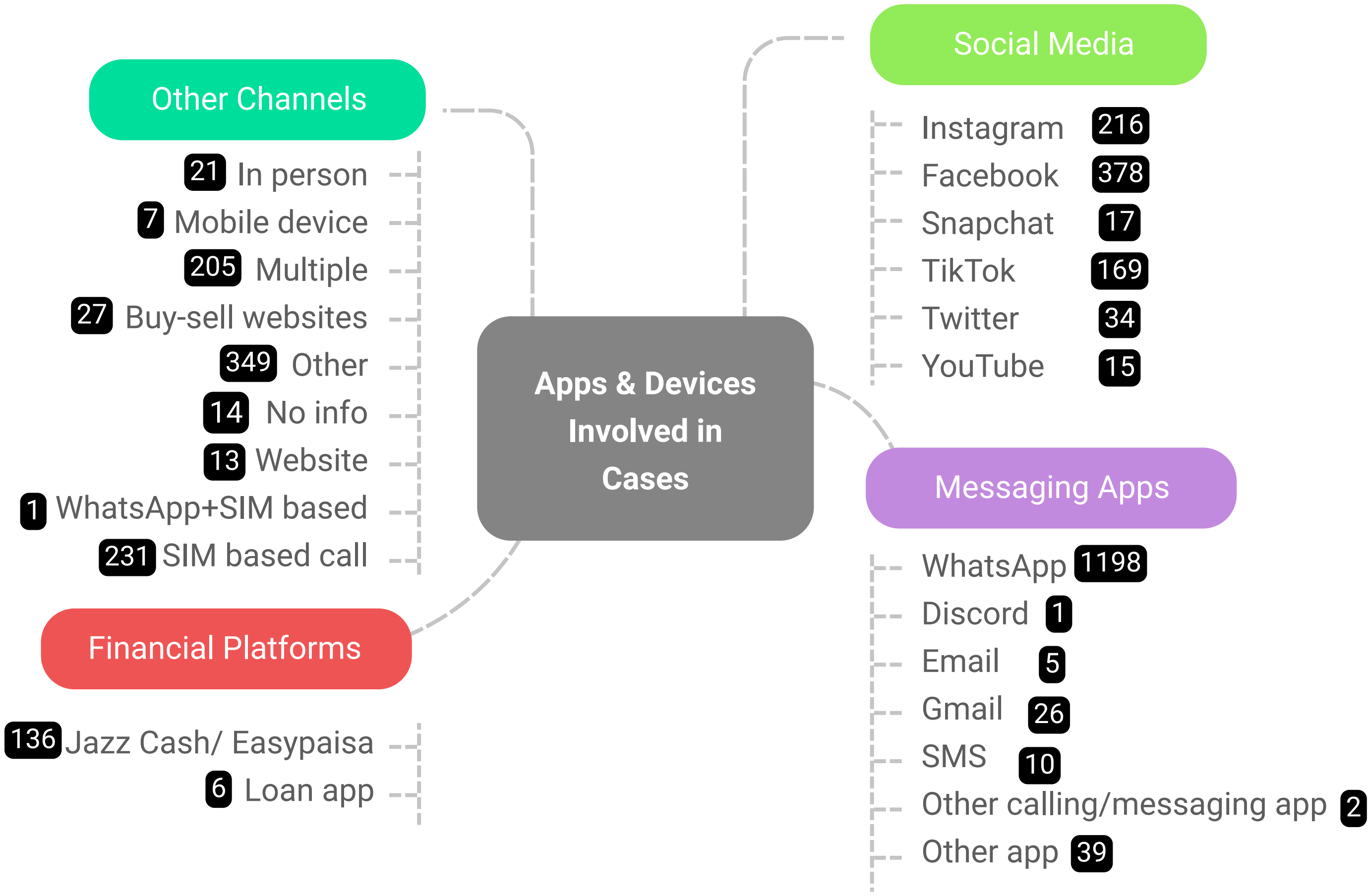


The Digital Security Helpline systematically monitors emerging patterns of online harassment and digital threats by analyzing the platforms where users report experiencing abuse. This data is instrumental in informing preventative strategies, equipping callers with digital safety guidance, and shaping public awareness campaigns to enhance online security. Additionally, these insights serve as a foundation for targeted advocacy efforts, enabling direct engagement with government agencies, social media platforms, and tech companies to push for policy reforms and enhanced safety mechanisms.

In 2024, WhatsApp, Facebook, and Instagram collectively accounted for 57.4% of reported cases, reflecting a 3% increase from the previous year. These platforms remain primary vectors for online harassment, emphasizing the urgent need for stronger, context-specific content moderation policies that prioritize user protection in high-risk regions.

To address this gap, the Helpline has established escalation channels and trusted partnerships with major platforms, advocating for improved policy enforcement and responsive safety tools. A one-size-fits-all, automation-dependent moderation model, designed primarily for English-language content and users in the Global North, often results in inadequate or excessive content moderation for cases emerging from South Asia and other Global Majority regions.

By maintaining regular dialogue with social media companies, the Helpline flags emerging digital threats, pressures platforms to adapt their policies for vulnerable users, and works proactively to mitigate online harm before it escalates into real-world consequences. As the Helpline expands its role as a regional digital security and incident response service, strengthening these collaborations and escalation mechanisms remains a top priority in ensuring safer digital spaces for all.



Apps & Devices Involved in Cases

Other Channels

- 21 In person
- 7 Mobile device
- 205 Multiple
- 27 Buy-sell websites
- 349 Other
- 14 No info
- 13 Website
- 1 WhatsApp+SIM based
- 231 SIM based call

Financial Platforms

- 136 Jazz Cash/ Easypaisa
- 6 Loan app

Social Media

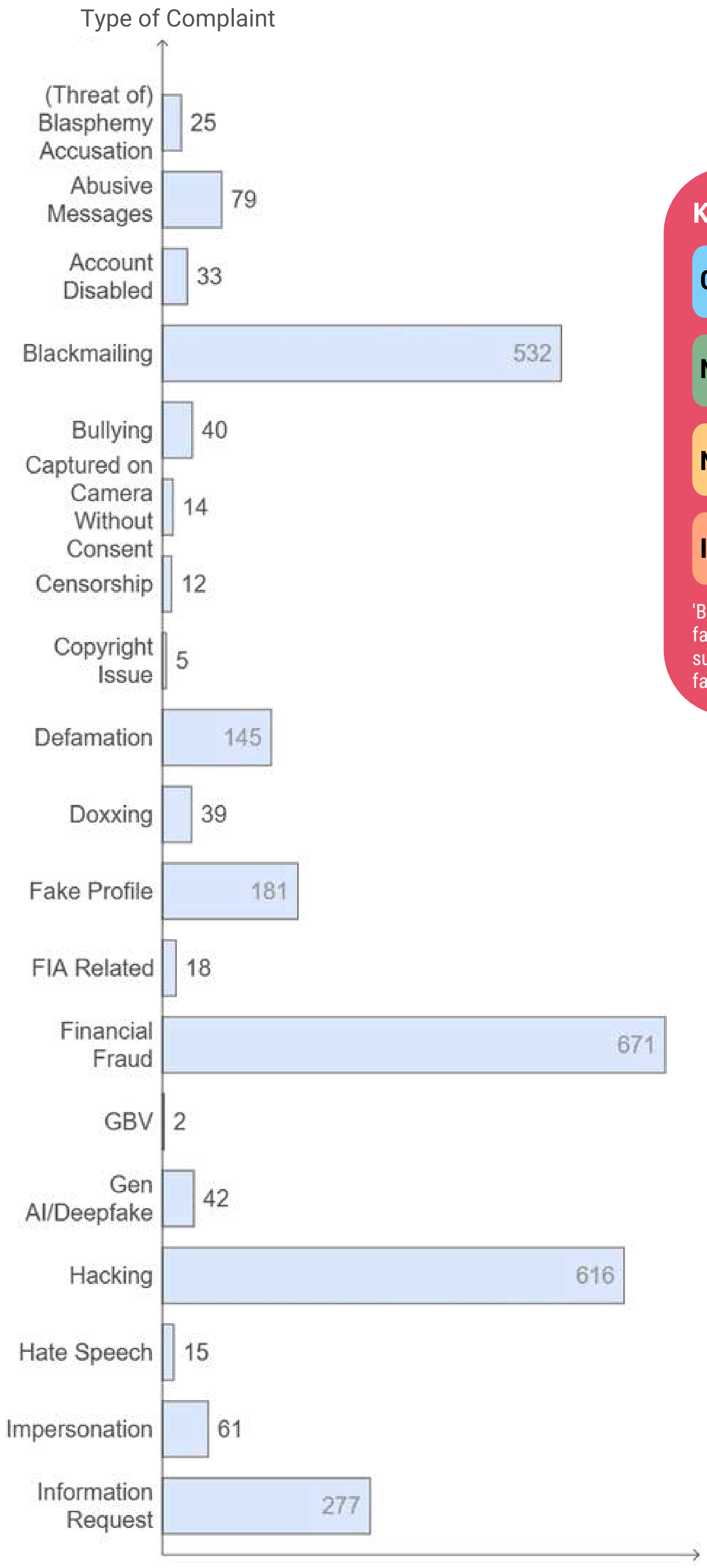
- Instagram 216
- Facebook 378
- Snapchat 17
- TikTok 169
- Twitter 34
- YouTube 15

Messaging Apps

- WhatsApp 1198
- Discord 1
- Email 5
- Gmail 26
- SMS 10
- Other calling/messaging app 2
- Other app 39

Gendered Patterns in Digital Threats: Key Trends and Insights

Type of Complaints Addressed

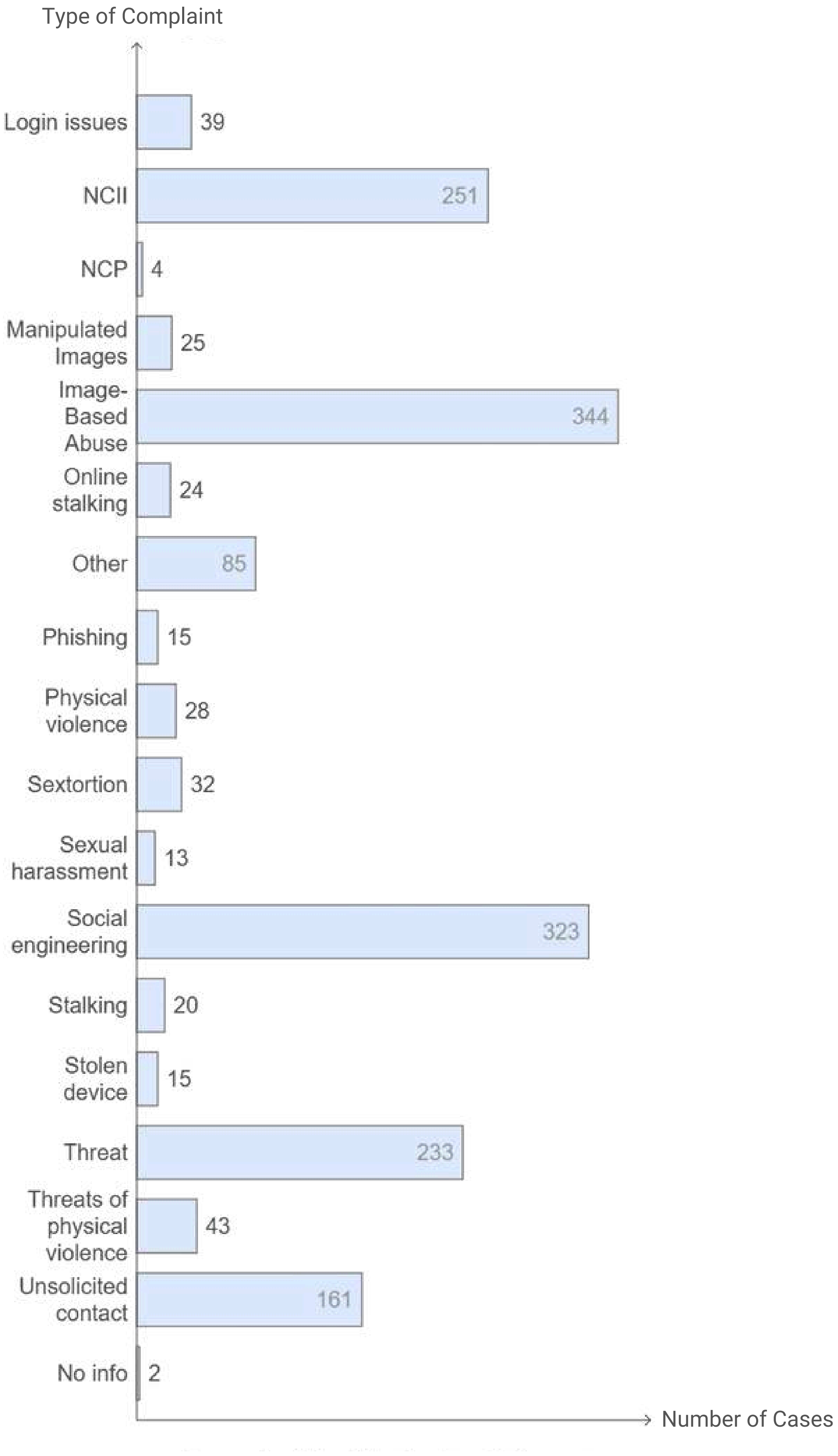


Key:

- **GBV** Gender-based violence
- **NCII** Non-consensual intimate images
- **NCP** Non-consensual pornography sent
- **IBA** Image-based abuse

'Blackmailing' may refer to asking for sexual or monetary favors in exchange for not distributing or tampering with a survivor's intimate images, or contacting the survivor's family

Type of Complaints Addressed (Contd.)



The Digital Security Helpline receives a diverse range of complaints, many of which follow gendered patterns in the way they manifest and impact individuals. While blackmail (including sextortion), hacking, threats, and unsolicited contact remain common concerns across all genders, women, men, and gender minorities experience these threats differently, often influenced by societal norms and power dynamics.

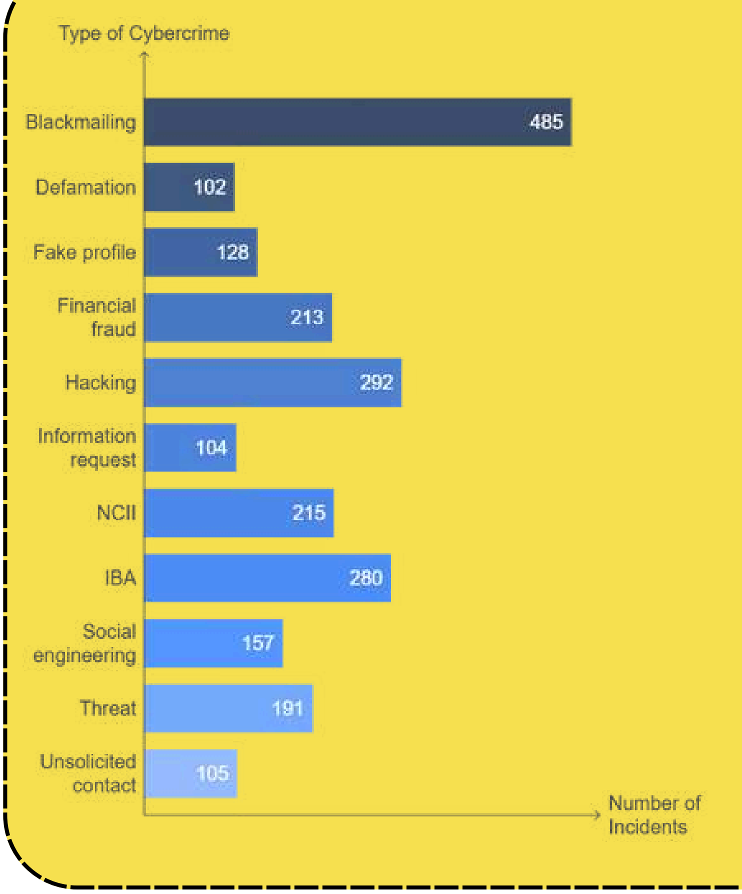
Women are disproportionately targeted with sexualized harassment, defamation, and non-consensual use of intimate images (NCII) and image-based abuse (IBA). These tactics exploit patriarchal honor-based norms and "honor-based" social structures, often aiming to control, shame, or coerce victims by threatening their reputation and familial relationships. Women also frequently report cases of blackmail, privacy breaches, and impersonation, with harassers using fear and social stigma as leverage to silence or manipulate them.

On the other hand, while men experience digital threats, such as blackmail, defamation, and fake profiles too, these incidents were less likely to involve sexualized content or honor-based threats as well. Instead, threats to men focused more on financial fraud, identity theft, hacking, or professional defamation, rather than reputation-based coercion. In many cases where reputation or personal defamation was a concern, men were targeted via questioning the honor of the women in their family.

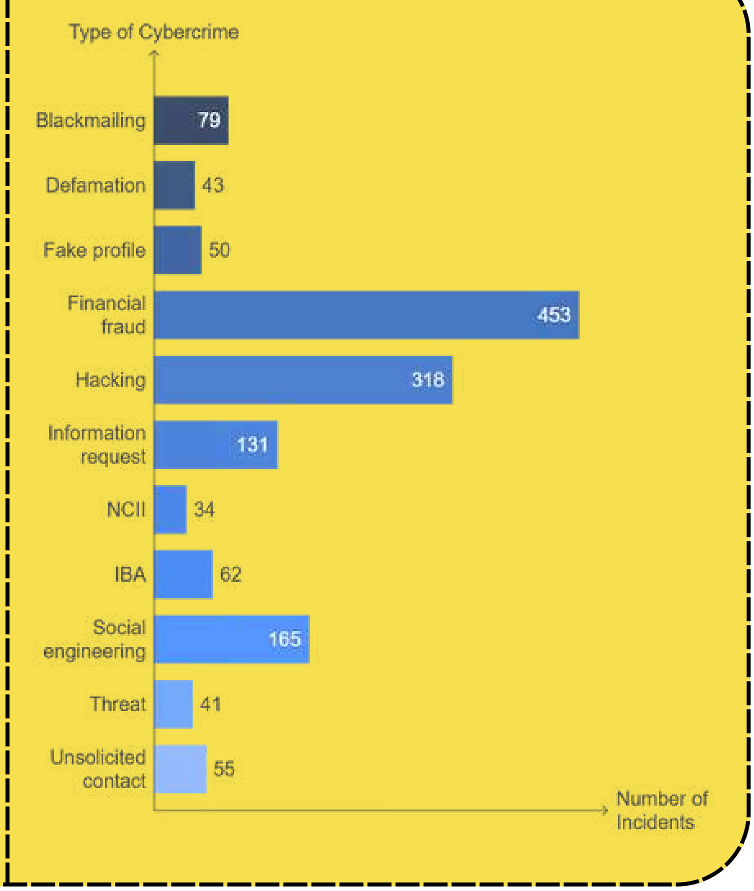
Furthermore, transgender individuals, non-binary persons, and other marginalized groups continue to face extreme levels of online abuse, including gendered disinformation, doxxing, and threats of physical harm, reflecting broader social discrimination and systemic exclusion.

Gender segregated types of complaints:

Women and trans women:



Men:



Note: Figures of blackmailing cases received include those involving sextortion

Since this was the first year when the Helpline recorded cases of deepfake intimate image abuse, we recorded such cases as a new, separate category; however, almost all except 3 cases involved AI generated intimate content, and so can be considered NCII as well. Many cases reported to the Helpline demonstrate the layered nature of digital abuse, where different forms of harassment overlap and escalate, creating long-term psychological, social, and financial consequences for victims.

Key insights:

- The data from this year shows that women are disproportionately targeted through NCII and IBA, with 85% of all NCII, and 81% of all IBA cases received targeting women; these methods are frequently used as forms of coercion, blackmail, and reputational damage. NCII/NCUI cases also frequently intersect with defamation and online impersonation.

- Blackmail often accompanies hacking and privacy breaches, with perpetrators weaponizing private data and personal communications. However, from our data, blackmailing is also deeply intertwined with sextortion and NCII. There were 196 instances which included elements of both NCII, and sextortion and blackmail.

- Women journalists, activists, and other public-facing professionals experience targeted harassment campaigns, where threats of violence and misinformation are used to silence their voices and professional credibility.

- Almost all sextortion complaints originated from women, revealing how coercion through explicit content remains a prevalent tactic.

- Women were far more likely to face targeted reputation damage, whether through false narratives, fake accounts impersonating them, or explicit image manipulation (e.g., deepfakes).

Content Takedown and Escalation Resolutions

The Digital Security Helpline has established escalation channels with multiple social media platforms to report harmful content and assist complainants. In cases where direct escalation is not possible, the Helpline takes independent action to request takedowns of content that violates laws or poses a significant risk to individuals. The reported content typically includes intimate or non-consensual images, fake or impersonation profiles, defamatory content, and account recovery requests for vulnerable and marginalized individuals.

In 2024, the Helpline made 197 escalations, observing notable trends and challenges. Meta platforms (Facebook, Instagram, and WhatsApp) accounted for the highest number of escalations (110 cases), followed by TikTok (48 cases), and Twitter (20 cases). Among these, TikTok exhibited the highest resolution rate, with cases being resolved in an average of just 3 days.

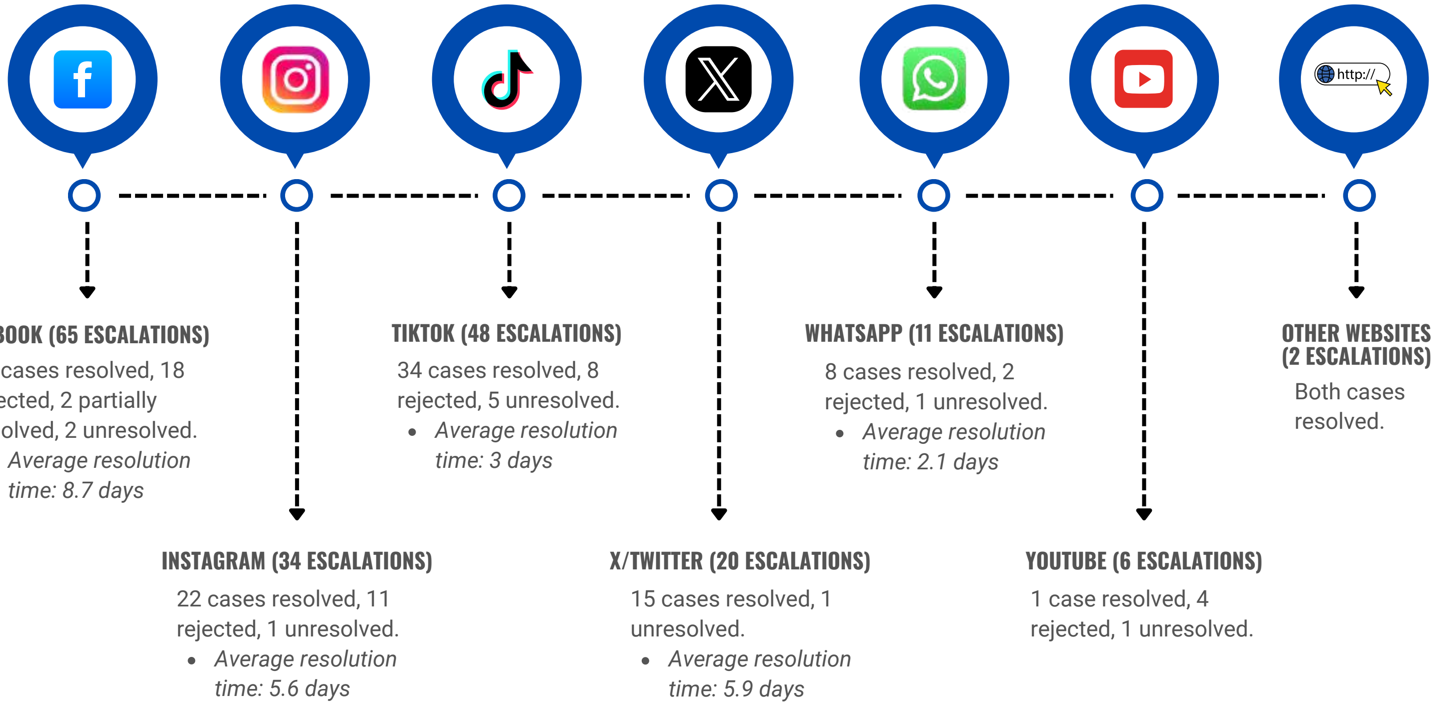
Despite ongoing engagement, many escalations remained unresolved. In multiple cases, platforms either failed to respond or provided generic instructions (such as asking complainants to fill out a form, which turns out to be successful only half the time) without fully resolving the issue.

Additionally, after the dismantling of X's escalation channel, the number of escalations, including pre-emptively highlighting mass trends, made by the Helpline dropped significantly.

A key concern continues to be platforms' inconsistent response patterns, including the time they take to respond. Response times varied between same day action, to several months, for all major platforms. The data from 2024 highlights gaps in platform responsiveness, especially regarding urgent cases involving gendered harassment, NCII, and impersonation. While some platforms, like TikTok, exhibited fairly quicker resolution times, others, like Meta and X and YouTube, require more accountability and structured engagement to ensure user protection.

It is pertinent to mention that while TikTok's resolution rate has been highest with quicker response rates as well, there have been many reservations by digital rights groups around their compliance with state demands. While DRF's Helpline would like to also do a comparative analysis of escalations made by the state to platforms, the current transparency reports by all platforms provide insufficient information to make that comparison.

Escalation of Cases To Social Media Platforms



FACEBOOK (65 ESCALATIONS)

43 cases resolved, 18 rejected, 2 partially resolved, 2 unresolved.

- *Average resolution time: 8.7 days*

INSTAGRAM (34 ESCALATIONS)

22 cases resolved, 11 rejected, 1 unresolved.

- *Average resolution time: 5.6 days*

TIKTOK (48 ESCALATIONS)

34 cases resolved, 8 rejected, 5 unresolved.

- *Average resolution time: 3 days*

X/TWITTER (20 ESCALATIONS)

15 cases resolved, 1 unresolved.

- *Average resolution time: 5.9 days*

WHATSAPP (11 ESCALATIONS)

8 cases resolved, 2 rejected, 1 unresolved.

- *Average resolution time: 2.1 days*

YOUTUBE (6 ESCALATIONS)

1 case resolved, 4 rejected, 1 unresolved.

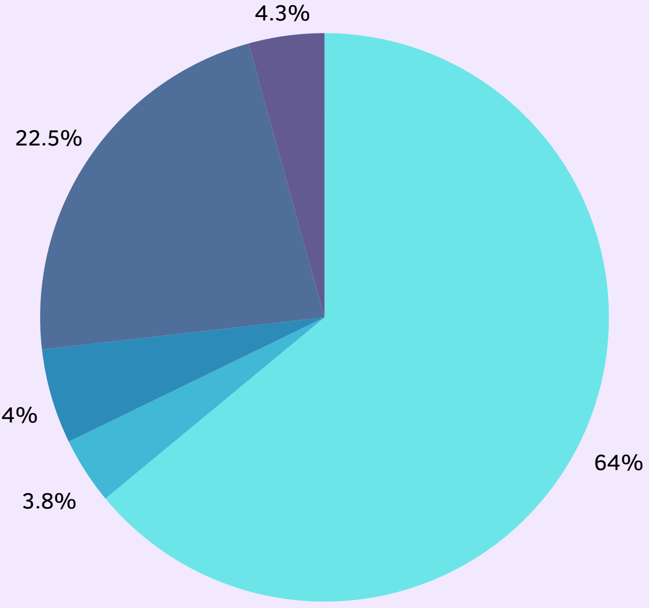
OTHER WEBSITES (2 ESCALATIONS)

Both cases resolved.

Making a Difference: The Helpline's Impact

To assess our effectiveness as a digital security and threat response helpline, we use multiple data sources to analyze case resolutions, evaluate service quality, and measure impact. Understanding how individuals discover the Helpline offers insight into our visibility and credibility:

- **64% of callers found us through social media**, highlighting the importance and effectiveness of our digital outreach.
- **3.8% were referred by a friend, family, or teacher**, indicating word-of-mouth trust in our services.
- **5.4% learned about us by directly reaching out to a DRF team member**, which demonstrates the strong networks that we have built over time with vulnerable communities.
- **22.5% of beneficiaries were referred by the police helpline**, which reflects our credibility, but also brings to light the number of people who face digital threats, yet are not equipped with the knowledge of how to report it.



Our strong online presence and digital word-of-mouth referrals reflect the trust and reliability associated with our support.

The number of incidents reported does not fully capture the Helpline's workload, as follow-ups are a significant part of our assistance. 23.5% of all calls (977 out of 4148) were follow-ups, highlighting our ongoing commitment and the considerable time we give to each case, to ensure the greatest possible resolution.

Out of all the threat incidents that came to the Helpline this year, 2791 (88%) were resolved from the Helpline's end. 9% of the cases received were left incomplete on the end of the beneficiary, so we are unable to ascertain whether the situation was resolved or not.

However, measuring impact can be complex due to our strict confidentiality protocols, because we do not initiate contact unless explicitly permitted, meaning we may not always receive updates. Furthermore, there may be subjective case resolutions; some beneficiaries may consider a temporary solution sufficient, while others require long-term monitoring.

To gather direct feedback, we conduct surveys with beneficiaries. However, this approach has limitations, such as small sample sizes, callers' varying access to technology, and incomplete responses based on individual understanding. We are actively refining our feedback collection methods to make them more inclusive, representative, and informative, ensuring that we continuously enhance our services based on real user experiences.

Impact Survey and Analysis

Q1. Which platform did you contact on?

Helpdesk email: 6 (15%)
Helpline: 20 (50%)
Social media: 13 (32.5%)
Not answered: 1 (2.5%)

Q2. How soon did you receive an initial response?

A few minutes: 24 (60%)
A couple of hours: 11 (27.5%)
1-2 days: 2 (5%)
Not answered: 3 (7.5%)

Q3. Do you identify as any of the following:

Activist: 1 (2.5%)
Civil society: 7 (17.5%)
Journalist: 9 (22.5%)
Lawyer: 1 (2.5%)
Karkun: 3 (7.5%)
Regular caller: 18 (45%)
Not answered: 1 (2.5%)

Q4. Did you receive any digital safety advice or help with digital/social media platforms?

Yes: 35 (87.5%) (includes situations where the case did not immediately need digital security assistance, but perhaps legal support)
No: 5 (12.5%)

Q5. Did the digital help you received reduce the risk you were facing?

Yes: 33 (82.5%)
No: 2 (5%)
Not answered: 5 (12.5%)

Q6: Did the digital assistance you received help in building short or long term capacity to protect yourself online?

Yes: 32 (80%)
No: 1 (2.5%)
Not answered: 7 (17.5%)

Q7: Did you receive digital advice beyond what was required at the time, e.g. tips to protect yourself in the future?

Positive: 11
Negative: 2
Not answered: 25

Q8: Did you receive any legal guidance or help with how to contact law enforcement?

Yes: 29 (72.5%)
No: 10 (25%)
Not answered: 1 (2.5%)

Q9: Did you choose to pursue legal action if necessary?

Yes: 21 (52.5%)
No: 15 (37.5%)
Not answered: 3 (7.5%)

Q10: Did you feel more confident seeking legal help after speaking with the Helpline?

Yes: 36 (90%)
No: 4 (10%)

Q11: If you spoke on the phone with a Helpline Associate, did you feel emotionally supported?

Yes: 36 (90%)
No: 2 (5%)
Maybe: 2 (5%)

Q12: Have you ever recommended the Helpline to someone else?

Yes: 25 (62.5%)
No: 12 (30%)
Not answered: 3 (7.5%)

Our beneficiaries' experience with the Helpline

> I had a comforting emotionally supported experience. Quick and secure experience. Really helped me alot. Great initiative for safe online experience. I will definitely recommend this platform to others

> I even went to Peshawar at cyber security office (FIA Cyber Crime Wing) but they didn't do anything at all, but Digital Rights Foundation did a great job and saved many lives...

> It was the only hope. I am glad I reached out to the Helpline. Will refer to others facing similar challenges

> Timely response and action helped a lot. On time, accurate scenario explanation. Forever grateful

In the face of emerging threats and evolving technology being used to put already vulnerable folks at risk, the Helpline ensured that the quality and efficiency of its services did not dip. We asked select beneficiaries:

Q1: Are you satisfied with the information provided by the Helpline?
Yes: 100%

Q2: Did you feel supported and encouraged after contacting the Helpline?
Yes: 100%

More feedback from our beneficiaries

> I was so miserable when I saw your post on facebook and I called in a heartbroken state not expecting anything but I am very grateful that you provided thorough guidance and helped me through this difficult time. May you, your work and your organization always prosper.

> Aapnay mera un halat m sath deeya hai jab meray apnay mera sath chor gaye hain. Main apki madad k leea hamaisha shukar guzar rahungi

> I was consoled by talking to the representative, my stress was lessened, you are doing a great work please continue doing it.

> 10/10 Satisfied with the assistance provided

Recommendations for Social Media Platforms

Social media platforms are key actors in shaping the safety and dignity of digital spaces. However, current moderation systems and escalation channels often fail to address the nuanced risks faced by vulnerable communities in the Global South. Based on insights from the cases received by the Digital Security Helpline, we propose the following recommendations:

Expand Context-Aware Moderation Across Borders
In countries like Pakistan, online content can have severe offline consequences, including social ostracization, violence, and even legal persecution. While some platforms do implement country-specific content moderation policies, such as restrictions on sensitive imagery or harmful narratives, these often fail to consider how harmful trends quickly spread across borders in regions with shared histories, languages, and cultural norms. Given the close proximity and intertwined socio-political dynamics of countries in South Asia, platforms must proactively evaluate whether policies developed for one country should be regionally applied. Expanding country-specific safeguards into broader regional frameworks could significantly reduce harm and prevent cross-border spillovers of digital abuse and disinformation.

Prioritize Escalations from Trusted Partners
Digital rights organizations such as DRF play a frontline role in addressing online abuse, and they understand the context, risks, and limitations faced by both platforms and users. Escalations submitted by trusted partners must therefore be prioritized, particularly in high-risk cases involving non-consensual image abuse, hate speech, impersonation, or sexualized threats, and the context they provide must be taken into strong consideration. From our experience, form-based or automated responses can create delays and worsen harm in crisis situations. Trusted Partner frameworks must be made more transparent, time-sensitive, and effective to ensure a mutually beneficial relationship.

Platforms must respond to escalation reports in a timely manner, without requiring informal outreach or direct messaging to platform representatives. Since Trusted Partners are already escalating content to platforms on a volunteer basis, the burden of additional nudges or reminders to initiate urgent action should not be on trusted partners alone. Platforms should proactively and transparently share relevant updates and changes with trusted partners, ahead of or alongside public announcements. Communications must be clear, context-specific, and action-oriented, rather than merely reiterating public press releases. In high-risk situations, delays in communication can significantly hinder timely response and support for survivors.

Trusted Partners often conduct substantial research and verification before submitting escalations. This involves navigating reporting system gaps, ensuring accuracy, and expending considerable time and human resources. When these well-substantiated reports are rejected without clear justification, the burden of re-engagement falls disproportionately on civil society. Platforms must recognize this effort and adopt a more accountable and responsive posture in their decision-making processes.

Ensure Continuity of Escalation Channels

Disruption in escalation mechanisms, such as the dissolving of X’s Trust and Safety Council, has left survivors without recourse. Platforms must ensure continuity and accountability in partner communication, especially during internal policy or staffing changes. Maintaining direct escalation contacts for local civil society partners is critical to ensuring user safety, especially in high-risk contexts. Recent political and industry developments have also created uncertainty among civil society about whether social media platforms remain committed to engaging meaningfully with Trusted Partners on issues of online safety and digital rights. However, these partnerships are essential for identifying local trends, responding to high-risk content, and ensuring that platform policies reflect regional realities. Measures must be taken to ensure that Trusted Partner programs are strengthened, rather than deprioritized.

Escalation Channels and Self-Reporting Tools

Based on the Helpline’s extensive experience, and the data we have presented earlier in this report, platforms must recognize the urgency which several cases demand. Hate speech, (indirect) blasphemy allegations, NCII, or even sensitive imagery can have severe consequences in this region, and delays in response or action jeopardize the safety of at-risk users. While some platforms (e.g., Meta) have improved their response times since 2020, much can be improved - an average response time of 5 to 9 days can still be harmful in certain cases with an imminent and direct threat. On the other hand, YouTube’s response rate and action standards have declined overall.

Several platforms have introduced escalation tools and forms, with the aim to standardize and regulate escalations. However, platforms should revise their moves towards limiting the scope of escalations, keeping in mind how different harms may affect users in different contexts and regions, and the ways in which bad actors exploit the gaps in policy implementations.

Furthermore, platforms also need to urgently improve the accessibility and responsiveness of their self-reporting tools. Some of the problems several beneficiaries have reported include not being able to access reporting forms, getting stuck in the middle of the process, not receiving a response, or receiving automated rejections, among others. This, coupled with reducing the scope of escalations, puts at-risk users at a dead-end.

Improve Transparency and Public Reporting

Platforms should publish disaggregated, country-level transparency reports detailing the nature of abuse reported, content takedown rates, resolution timelines, and escalations accepted or rejected, whether from civil society partners or governments. Transparency is especially vital when harm involves gender minorities, journalists, or survivors of TFGBV.

Adapt AI Moderation Tools for Regional Use

Automated content moderation systems routinely miss context-specific risks; they also censor journalists and media organizations working in regional languages, and reduce their monetization and reach. Platforms must invest in building inclusive training datasets and moderation tools capable of understanding regional language, nuance, and threat patterns. Harmful content embedded in religious, ethnic, or gendered rhetoric, particularly in images and videos, often slips past current systems, increasing risk for marginalized users.

Co-create Educational Resources

Safety information should be accessible and locally relevant. Platforms should work with regional partners to develop privacy guides, reporting tools, and anti-harassment resources tailored to different regions in the Global South, especially for women, youth, and transgender communities. These materials should be available in local languages and formats accessible to users with low literacy or digital literacy. Learnings from the focus groups that DRF held with parents of teens and tweens indicate that parents were largely unaware of the safety tools introduced by platforms, and needed detailed guidance on how to apply the tools to their situations.

Design for Discretion and Safety

Product design must consider the unique risks of surveillance and coercion in South Asian households. Safety tools such as anonymous reporting, comment moderation, privacy toggles, and disappearing messages should be designed to enhance user autonomy, especially for survivors of abuse accessing the internet through shared or monitored devices.

Engage in Ongoing Regional Consultations

Platforms should institutionalize regular engagement with civil society in the Global South, particularly South Asia. These consultations should inform safety policy updates, escalation procedures, product development, and crisis response planning, ensuring that the lived experiences of vulnerable users directly shape platform governance. Platforms should also note that enforcing policy changes to influential Global North regions (such as the USA) will certainly have an effect on Global Majority regions, putting users here at further risk, for example, through the extension of harms caused by disinformation and reduced credibility of fact-checking services.

Recommendations for Policymakers

Consistency, Clarity, and Approachability

Over the past year, numerous changes related to PECA and its enforcement have been proposed and approved. Any modifications to the complaint-filing process should prioritize accessibility, ease, and efficiency for those affected by cybercrimes, particularly women and marginalized groups. Rather than introducing abrupt structural changes, such as the formation of a new investigative body, its subsequent dismantling, and now the proposal for another new body, it would be more effective to address the root causes and systemic challenges that both complainants and law enforcement officials have identified as obstacles to investigations and case resolution. Investing in the resources, training, and technical and forensic capabilities of existing law enforcement agencies would likely yield greater efficiency and effectiveness.

Public Education & Digital Literacy

To effectively address online harassment and TFGBV, the Pakistani government must invest in public education and digital literacy initiatives. A gender-sensitive approach should be incorporated into school curriculums, public awareness campaigns, and community programs to ensure that young people understand online consent, social media ethics, cyber laws, and digital safety. Partnering with gender and digital rights organizations will help ensure that these efforts are inclusive and responsive to the challenges faced by women and marginalized groups. Regular updates to the curriculum should reflect emerging threats and technological advancements to keep students well-informed about online risks.

Bridging the Digital Gender Divide

Pakistan has one of the world’s largest digital gender gaps, with women 35% less likely than men to own a mobile phone due to financial constraints, patriarchal attitudes, and safety concerns (GSMA 2024). Bridging this divide requires targeted policies that make digital access more affordable and inclusive. The government should work with mobile network operators to introduce subsidized mobile internet packages for women and ensure that underserved regions receive improved internet infrastructure. Additionally, social barriers must be addressed by challenging restrictive norms that limit women's digital participation. A combination of awareness campaigns, community engagement, and economic incentives can help create an environment where women feel safe and empowered to access the internet freely.

Gender-Sensitive Law Enforcement

Law enforcement agencies must adopt a survivor-centered approach when handling cases of cyber harassment. Regular gender sensitization training should be mandatory for all officers, particularly those within the FIA and police departments. These sessions should cover the unique challenges faced by women and gender minorities in online spaces, ensuring that officers handle complaints with empathy and professionalism. Collaborating with civil society organizations like DRF, which has previously conducted such training for the FIA's cybercrime wing, will help standardize best practices. Additionally, mechanisms for monitoring and evaluating these training programs must be put in place to ensure that gender sensitivity becomes an integral part of law enforcement culture rather than a one-time initiative.

Strengthening Data Protection Laws

Pakistan must enact comprehensive and human rights-compliant data protection legislation that safeguards citizens' privacy and digital security. Current gaps in legal frameworks leave individuals vulnerable to unauthorized data collection, breaches, and misuse. To address this, the government should conduct meaningful consultations with civil society organizations before drafting legislation, ensuring alignment with international best practices. The right to privacy, enshrined under Article 14 of Pakistan's Constitution, must be upheld through clear guidelines on data collection, processing, and sharing. Citizens must also have access to legal recourse in case of privacy violations, with strict penalties enforced against data misuse. Additionally, mechanisms should be put in place to ensure transparency and accountability in how government agencies handle personal data.

Supporting Civil Society & Digital Rights Advocacy

The government must ensure an enabling environment for civil society organizations working on digital rights and gender equality. Restrictions on civil society and advocacy groups must be lifted to allow for meaningful engagement on issues related to online harassment, digital privacy, and cybercrime. Additionally, financial and institutional support should be provided to organizations conducting research, policy advocacy, and survivor support services. Meaningful collaboration between policymakers and civil society will help bridge gaps in service delivery and ensure that digital rights remain a national priority.

Recommendations for Law Enforcement Authorities

Increasing Resource Allocation & Technical Capacity

The FIA (or any new investigative body) must receive increased funding to meet the rising demand for cybercrime investigations. With TFGBV cases on the rise, additional resources should be allocated to expand forensic labs, hire and train more female officers, and improve response mechanisms. Given the rapid evolution of cyber threats, officers must receive continuous technical training in digital forensics, evidence collection, and emerging online crime trends. Collaboration with international partners will help improve investigative capabilities, ensuring that Pakistan's law enforcement agencies remain equipped to handle complex cybercrime cases effectively.

Addressing Cases in Foreign Jurisdictions

Many cybercrime cases involve perpetrators outside Pakistan, yet the FIA lacks the capacity to take legal action against them. While Section 1(4) of the Prevention of Electronic Crimes Act (PECA) gives the FIA the authority to handle cross-border cybercrimes, practical enforcement remains a challenge. To address this, the government must clarify the definition of "international cooperation" under Section 42 of PECA and appoint specialized officers in each branch trained in international law. Strengthening diplomatic channels for cybercrime cooperation will help expedite legal actions against perpetrators operating beyond Pakistan's borders.

Enhancing the Online Complaint Portal

The FIA's online complaint portal must be upgraded to improve accessibility and efficiency. Many complainants, especially women, are unable to travel long distances to file cybercrime reports. An improved portal should include identity verification mechanisms to initiate inquiries online, allowing victims to seek justice without facing unnecessary bureaucratic hurdles. Additionally, the portal should provide comprehensive information on available legal options, survivor support services, and case tracking features to keep complainants informed about the status of their cases. Many complainants have also communicated that the FIA is unreachable by phone and so they are unable to get relevant information before traveling; accessibility in all its different forms should be prioritized.

Improving Coordination Between Police & Cybercrime Units

The recent PECA amendments allow local police stations to handle cybercrime-related cases in cities where the FIA is not present. To ensure that survivors receive the necessary support, the FIA must develop clear protocols guiding police officers on how to process cybercrime complaints with empathy and efficiency. Police departments should appoint focal persons dedicated to handling cybercrime cases who are well-versed in cybercrime trends and are able to provide guidance on and resolve basic cybercrimes. These focal persons should ensure better coordination between the FIA and local law enforcement, which will help reduce jurisdictional confusion and prevent survivors from being sent back and forth between agencies while seeking justice.

Collecting Gender-Disaggregated Data on Cyber Harassment

To improve policy responses to TFGBV, the FIA must publicly report gender-disaggregated data on cyber harassment cases. Data collection should be standardized under PECA, particularly for cases filed under Sections 20, 21, and 24, which address online defamation, harassment, and non-consensual sharing of intimate images. Transparent reporting on the number of cases registered by women and gender minorities will help policymakers and researchers develop more effective interventions to address online violence.

Establishing a Dedicated Cyber Harassment Unit

Given the unique nature of cyber harassment cases, the FIA must set up a separate unit within the National Response Centre for Cyber Crimes (NR3C) dedicated to handling online gender-based violence. This unit should be staffed by officers with specialized training in digital harassment, trauma-informed response, and survivor support. A dedicated cyber harassment unit will ensure that victims receive timely, sensitive, and effective responses to their complaints.

Ensuring Privacy & Confidentiality for Survivors

Many complainants hesitate to report cyber harassment due to fears of retaliation and breaches of confidentiality. Rule 9 of the PECA Rules outlines protections for women's privacy in online harassment cases, yet implementation remains weak. The FIA must strengthen its internal case management system to ensure that personal data, case details, and digital evidence are securely stored and accessible only to authorized personnel. A secure digital case tracking system will help prevent unauthorized access to sensitive information while maintaining survivors' trust in law enforcement.

Enhancing Accessibility for Disabled Complainants

Cybercrime offices must be made accessible to individuals with disabilities. Many complainants face additional hurdles due to the lack of functioning elevators, wheelchair ramps, and accessible restrooms. Ensuring that all cybercrime offices meet basic accessibility standards will help disabled individuals report cases without unnecessary obstacles.

Improving Coordination Between Cybercrime Branches

Investigations are often delayed when the complainant and the accused reside in different cities, leading to inefficiencies in case handling. The FIA must evaluate its regional branches to ensure standardized procedures are followed across all locations. A centralized database for cybercrime cases should be established to streamline inter-branch coordination and reduce delays in evidence collection and suspect apprehension.

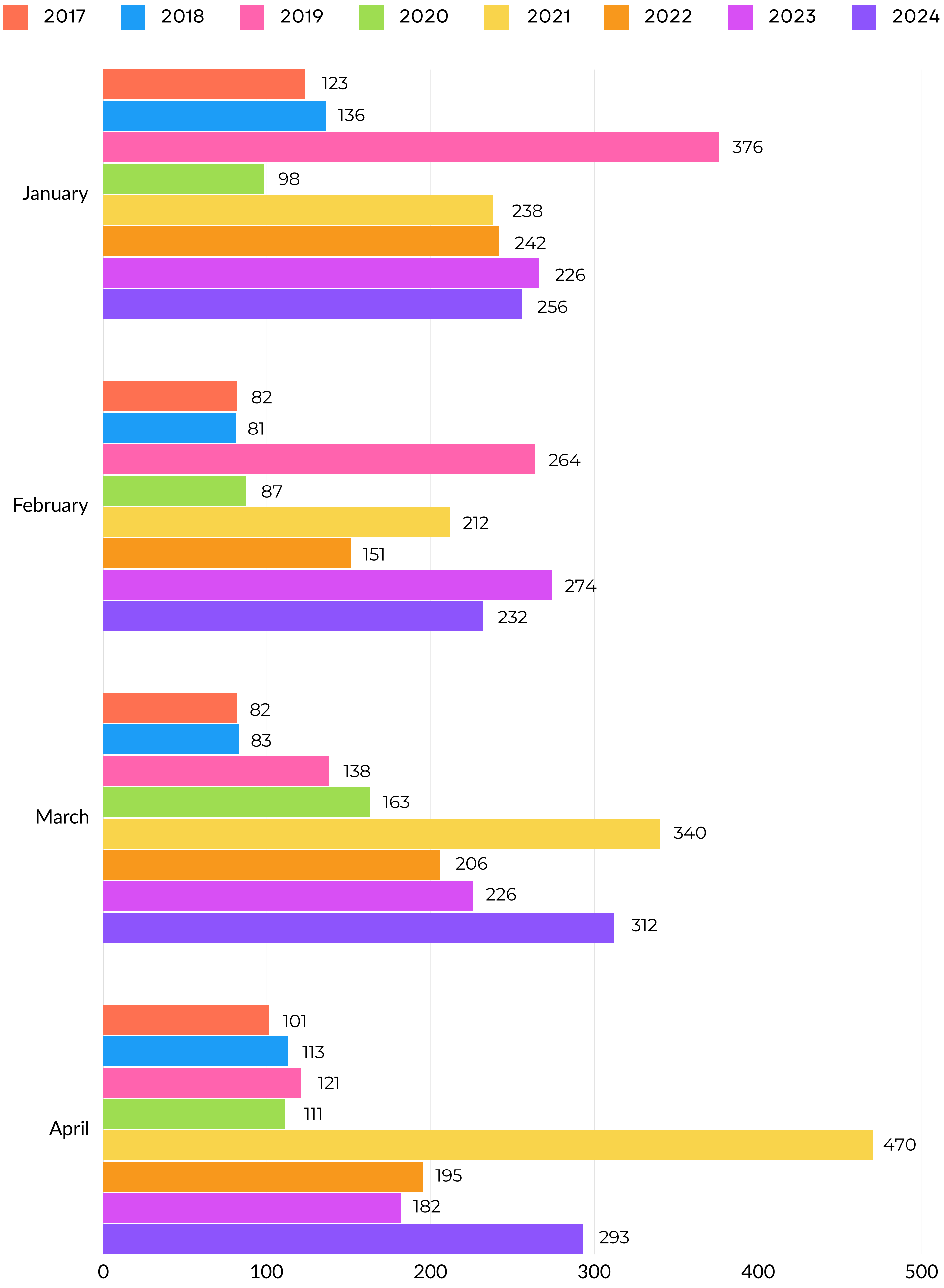
Providing Psychological Support Services

Online harassment survivors often experience severe emotional distress. The FIA must integrate psychological support services within cybercrime units, offering trauma counseling to complainants. Officers handling cyber harassment cases should be trained in trauma-informed response techniques, ensuring that victims receive compassionate and professional support.

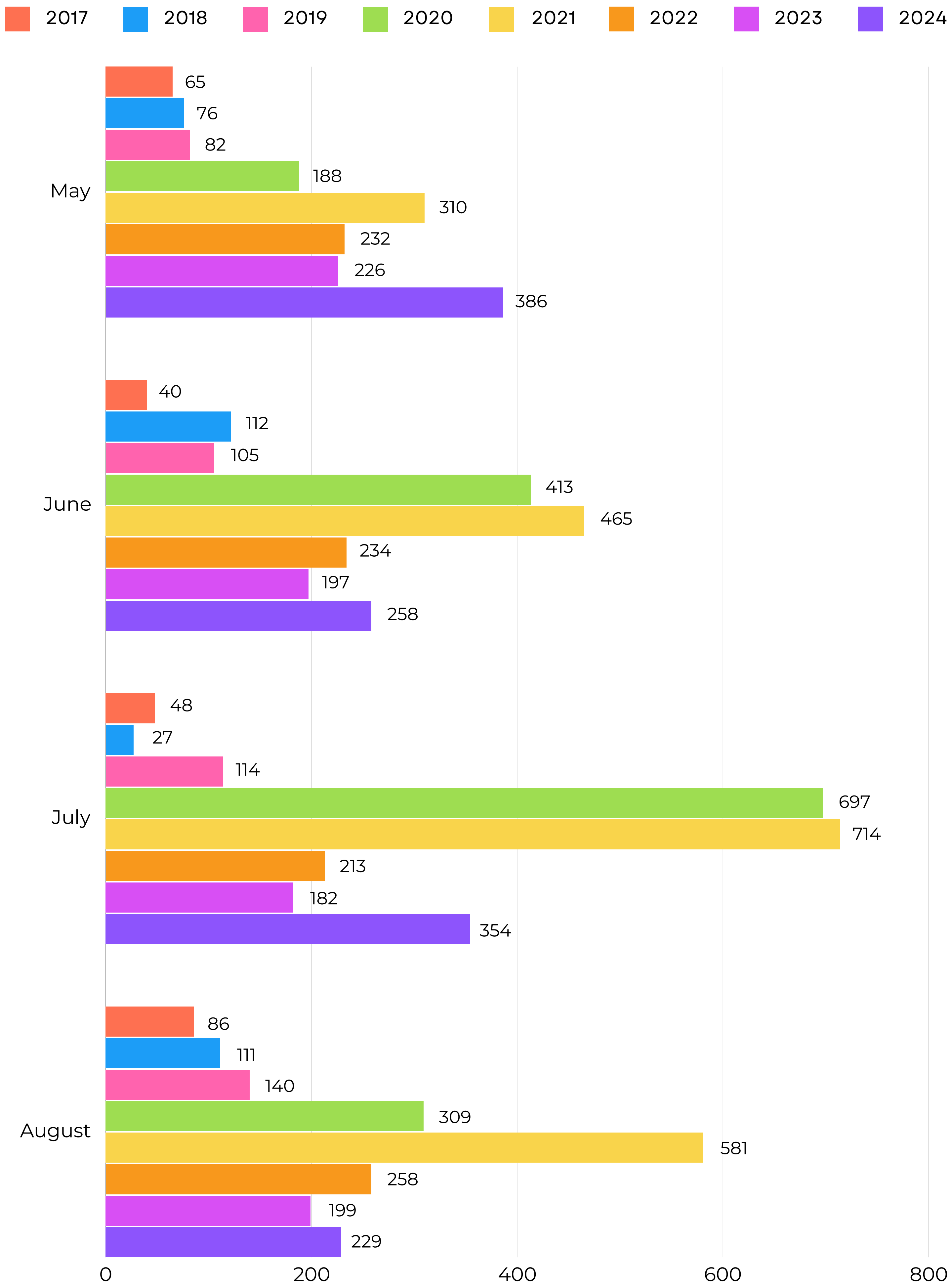
Implementing a Case Tracking System

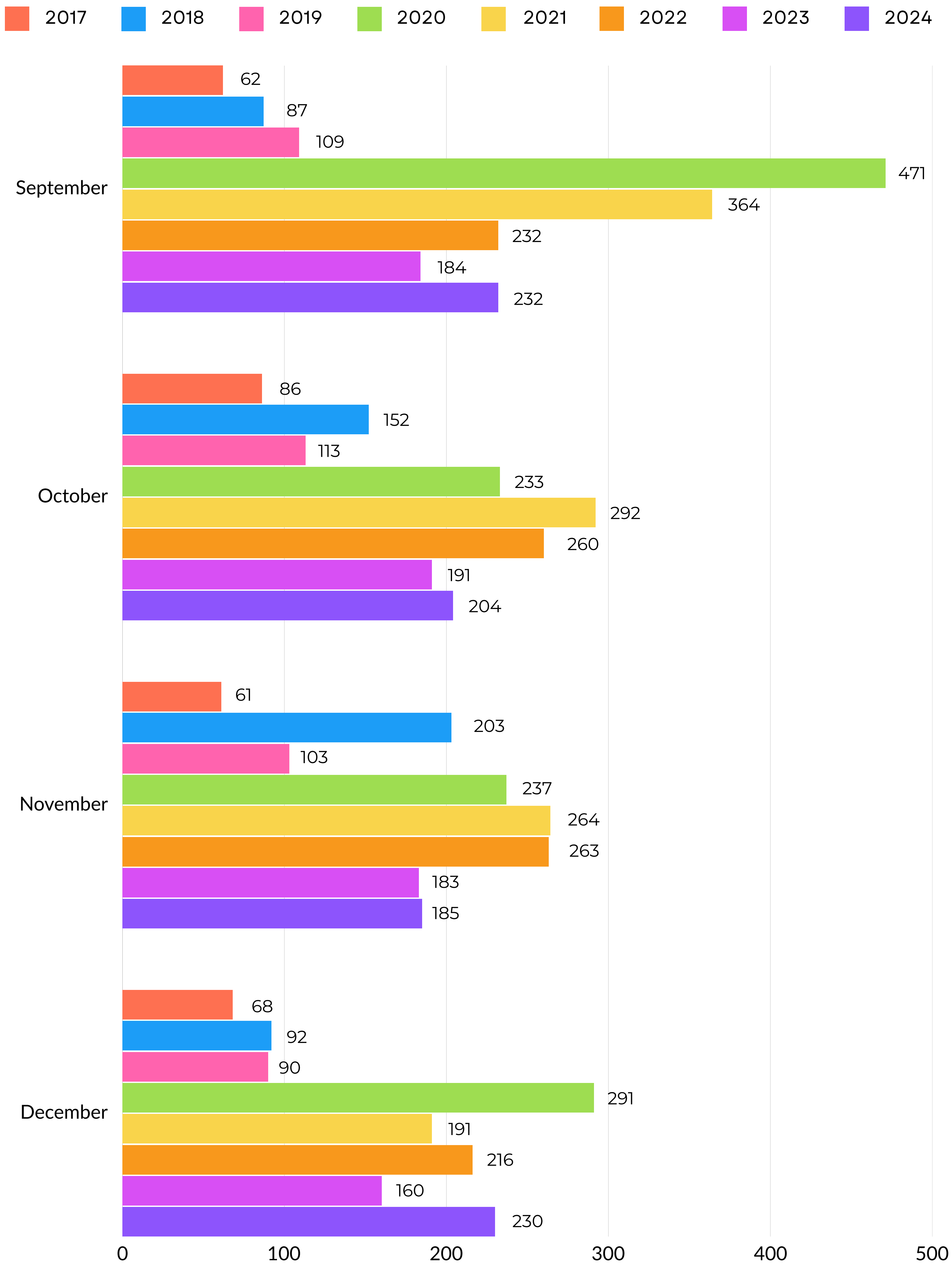
To improve transparency and trust in law enforcement, complainants should have access to a digital case tracking system where they can monitor the progress of their complaints. Secure digital copies of case files and evidence should be maintained to prevent case mismanagement and loss of crucial data.

Appendix 1



2017
2018
2019
2020
2021
2022
2023
2024
January
123
136
376
98
238
242
226
256
February
82
81
264
87
212
151
274
232
March
82
83
138
163
340
206
226
312
April
101
113
121
111
470
195
182
293
0
100
200
300
400
500


2017
2018
2019
2020
2021
2022
2023
2024
May
65
76
82
188
310
232
226
386
June
40
112
105
413
465
234
197
258
July
48
27
114
697
714
213
182
354
August
86
111
140
309
581
258
199
229
0
200
400
600
800


2017
2018
2019
2020
2021
2022
2023
2024
September
62
87
109
471
364
232
184
232
October
86
152
113
233
292
260
191
204
November
61
203
103
237
264
263
183
185
December
68
92
90
291
191
216
160
230
0
100
200
300
400
500

DigitalRightsFoundation

"KNOW YOUR RIGHTS"

@DigitalRightsFoundation

@digitalrightsfoundation

@digitalrightsfoundation

@digitalrightsfoundation

Digital Rights Foundation

@digitalrightspk.bsky.social

@DigitalRightsPK

@DigitalRightsPK

digitalrightsfoundation.pk