

First Quarter Sextortion Case Monitoring Report

January – April 2026

Ghana Internet Safety Foundation (GISF)

www.gisfoundation.com

Publication Information



Organization: Ghana Internet Safety Foundation (GISF)

Reporting Period: January – April 2026

Publication Date: May 2026

Report Type: Quarterly Case Monitoring and Trend Analysis Report

Prepared By: Ghana Internet Safety Foundation – Online Safety and Victim Support Team

Confidentiality Classification: Public Version (Anonymized)

Version: 1.5

Table of Contents

1. Executive Summary	4
2. Introduction	7
3. Definitions and Scope	10
4. Objectives of the Report.	12
5. Legal and Policy Framework	14
6. Methodology	17
7. Ethical Reporting and Data Protection Statement	20
8. Data Overview	22
9. Monthly Case Distribution	24
10. Gender Distribution	26
11. Age Distribution	28
12. Platforms Used	30
13. Case Classification and Emerging Trends.	32
14. January Case Insights	35
15. April Case Insights	37
16. Perpetrator Tactics and Modus Operandi.	39
17. Impact on Victims	41
18. Reporting Channels Analysis	43
18A. National CyberTip and Hotline-Linked Trends in Ghana (Ghana Police Service)	45
19. Key Observations.	49
20. Key Observations and Challenges	52
21. Safeguarding and Survivor Protection Considerations	54
22. Evidence Preservation and Incident Response Guidance.	56
23. Recommendations and Future Priorities	58
24. Conclusion	60
25. Limitations of the Report	62
26. Conclusion	64
27. Appendix - Anonymized Case Summaries	66

Executive Summary

1.0 Executive Summary

This report presents a consolidated analysis of sextortion-related cases reported between January and April 2026 through the Ghana Internet Safety Foundation's reporting and support channels.

The report was developed to support awareness creation, policy engagement, victim support discussions, and broader national conversations on online safety and digital harm prevention in Ghana. It also contributes to ongoing efforts to better understand evolving sextortion patterns affecting internet users, particularly young people in Ghana who are highly active on social media and messaging platforms.

A total of 120 online harm and sextortion-related cases were recorded during the reporting period. January recorded 58 cases, representing 48.3% of all documented incidents, while April recorded 62 cases, representing 51.7% of the total reported cases during the reporting period.

Approximately 40% of all reported incidents involved Child Online Protection (COP)-related concerns, including sextortion attempts targeting minors, cyberbullying, online grooming indicators, non-consensual sharing of images involving minors, online harassment among students, and threats linked to intimate content.

Among the COP-related reports, the majority of affected victims fell within the Senior High School age bracket of approximately 15–18 years, while the remaining cases involved upper primary and junior high school-aged children between approximately 10–14 years. These findings reinforce growing concerns regarding the vulnerability of school-aged children and adolescents to online exploitation and abuse.

The cases reflected a broader range of online harms extending beyond traditional sextortion. Reported incidents included financial sextortion, cyberstalking, romance scam-related exploitation, account compromise, unauthorized sharing of intimate content, impersonation, online harassment, emotional coercion, blackmail, and privacy-related abuses.

The increase in reports during January and April may reflect heightened awareness, increased visibility of reporting channels, and growing public willingness to seek help regarding online abuse and exploitation incidents.

Out of the 120 reported cases, approximately 86 victims were females, representing 71.7% of all reported cases, while approximately 34 victims were males, representing 28.3%. This indicates that females were disproportionately affected during the reporting period, although males also remain vulnerable to sextortion-related exploitation.



Emmanuel Adinkra

President

Ghana Internet Safety Foundation

The age distribution of victims further highlights the vulnerability of young internet users. Approximately 46% of all documented victims fell within the 18–25 age category, while approximately 40% involved children and adolescents linked to Child Online Protection concerns. The remaining cases involved adults above 25 years. These findings highlight the heightened vulnerability of younger internet users, students, and active social media participants. This suggests that young adults, particularly active social media users, remain primary targets of sextortion perpetrators.

The report also identified WhatsApp as the dominant platform linked to reported incidents, accounting for approximately 58% of all documented cases. Snapchat, Facebook, and TikTok were also associated with reported incidents during the reporting period. The findings reinforce wider global concerns regarding the misuse of social networking and messaging platforms for exploitation, blackmail, and emotional coercion.

The increase in reporting activity during January and April may reflect increased awareness, improved visibility of reporting channels, and greater willingness among victims to seek support regarding online harms and sextortion-related abuse.

A key operational finding is that 100% of valid cases were reported through the Foundation’s dedicated call line, while the GISF Hotline 267 system recorded limited valid sextortion-related reports during the reporting period. This was largely due to misuse, wrong-number calls, operational inefficiencies, and unrelated inquiries.

The report further demonstrates that sextortion incidents often involve emotional manipulation, fake identities, secret recording of intimate calls, financial extortion, hacking, cyberstalking, and threats to publicly release intimate content. Financial demands in reported cases ranged between GHC 400 and GHC 5,000.

The findings underscore the need to:

- Strengthen awareness campaigns
- Improve reporting systems and hotline effectiveness
- Enhance data collection processes
- Promote trusted reporting channels
- Improve safeguarding and survivor support mechanisms
- Strengthen collaboration with law enforcement, educators, platforms, and mental health professionals
- Encourage digital literacy and safer online behavior

This report should not be interpreted as a measure of national prevalence. Rather, it represents documented cases received through GISF’s reporting mechanisms during the reporting period. The findings nevertheless provide important insight into emerging trends, operational gaps, and areas requiring urgent intervention within Ghana’s online safety ecosystem.



Introduction

2.0 Introduction

Sextortion is a form of online exploitation where perpetrators threaten to release private, intimate, or sexually explicit content unless victims comply with demands such as money, additional explicit content, continued communication, or other actions.

Globally, sextortion continues to emerge as a major online safety and digital rights concern affecting young people, women, vulnerable adults, and increasingly male victims. Social media platforms, online dating environments, messaging applications, and video calling platforms are frequently exploited by perpetrators to manipulate victims emotionally, financially, and psychologically.

The increasing accessibility of smartphones, social media applications, encrypted messaging platforms, and digital communication tools has significantly changed the nature of interpersonal relationships and online interactions. While these technologies create opportunities for communication and social connection, they have also created new pathways for abuse, exploitation, harassment, and blackmail.

In many sextortion cases, perpetrators exploit emotional trust, loneliness, peer pressure, curiosity, or romantic interest to manipulate victims into sharing intimate content or participating in intimate video interactions. In other cases, perpetrators may obtain intimate material through hacking, unauthorized access to devices, or misuse of personal information.

The emotional and psychological impact of sextortion can be severe. Victims may experience fear, shame, anxiety, depression, social withdrawal, reputational harm, financial loss, and trauma. In extreme situations, victims may express suicidal thoughts or self-harm ideation due to fear of exposure and public humiliation.

The Ghana Internet Safety Foundation established multiple reporting and support channels to encourage safer reporting, provide guidance to victims, and improve visibility into emerging online harm trends.

Reporting channels during the reporting period included:

- GISF Hotline 267 (MTN network)
- Dedicated call line (0545957408)
- WhatsApp anonymous messaging channel
- Direct messages through official social media accounts



This report combines case monitoring data and reporting channel performance analysis to provide a broader overview of trends, patterns, risks, operational gaps, and recommendations relating to sextortion incidents reported between January and April 2026.

The report also seeks to support public awareness, advocacy, prevention efforts, and stakeholder engagement on online safety and digital harm prevention in Ghana.

Beyond case analysis, the report aims to contribute to broader national conversations on digital literacy, responsible technology use, safeguarding, and the importance of trusted reporting systems. It is also intended to support policymakers, educators, civil society organizations, mental health professionals, researchers, law enforcement agencies, and online safety stakeholders seeking to better understand the evolving nature of sextortion-related abuse.

Definitions and Scope

3.0 Definitions and Scope

For the purposes of this report:

Sextortion refers to a form of exploitation where perpetrators use intimate or sexually explicit content, or the threat of releasing such content, to coerce victims into providing money, additional content, sexual favors, or continued engagement.

Financial Sextortion refers to cases where perpetrators demand money in exchange for not releasing intimate material.

Image-Based Abuse refers to the non-consensual sharing, threat of sharing, or misuse of intimate images or videos.

Romance-Related Sextortion refers to cases where perpetrators build emotional or romantic trust before coercing victims.

Cyberstalking and Harassment refers to repeated intimidation, threats, monitoring, or online harassment targeting victims.

This report focuses on cases voluntarily reported to GISF through available reporting channels between January and April 2026.

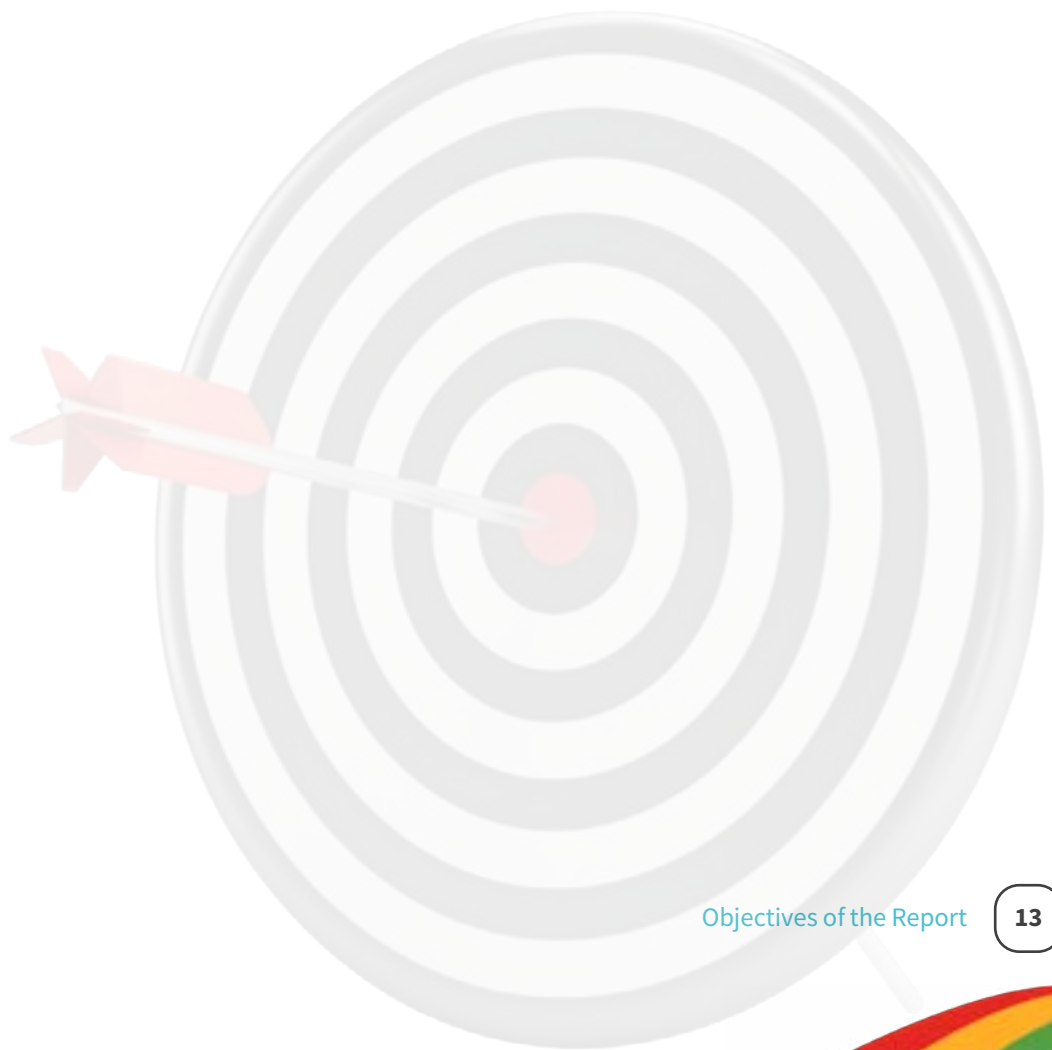
The report includes adult victims only based on the available data collected during the reporting period. The report does not seek to determine criminal liability and should not replace formal law enforcement investigations.

Objectives of the Report

4.0 Objectives of the Report

The objectives of this report are to:

- Analyze sextortion cases reported between January and April 2026
- Identify trends, patterns, and emerging tactics
- Evaluate the effectiveness of existing reporting channels
- Highlight safeguarding and victim support concerns
- Support advocacy and awareness efforts
- Inform policy, prevention, and stakeholder engagement initiatives
- Provide actionable recommendations for improving response systems





Legal and Policy Framework

5.0 Legal and Policy Framework

This report is informed by Ghana's existing legal and policy environment relating to cybercrime, online abuse, privacy, and digital safety.

Relevant national frameworks include:

- Cybersecurity Act, 2020 (Act 1038)
- Data Protection Act, 2012 (Act 843)
- Criminal Offences Act, 1960 (Act 29)
- Electronic Transactions Act, 2008 (Act 772)
- Domestic Violence Act, 2007 (Act 732)
- Child and Family Welfare Policy
- National Child Online Protection Framework

Publicly accessible references and resources include:

- Cybersecurity Act, 2020 (Act 1038):
<https://repository.parliament.gh/items/3a888118-9a6e-4c6c-ba35-c41c971ec1bc> (repository.parliament.gh)
- Cyber Security Authority Ghana Resources:
<https://www.csa.gov.gh/resources.php> (csa.gov.gh)
- Data Protection Commission Ghana:
<https://dataprotection.org.gh/> (dataprotection.org.gh)
- Data Protection Act, 2012 (Act 843) overview:
https://en.wikipedia.org/wiki/Data_Protection_Act%2C_2012 (en.wikipedia.org)
- WHO legal repository reference for Data Protection Act, 2012 (Act 843):
<https://extranet.who.int/cpcd/health-legislation/data-protection-act-2012-act-843> (extranet.who.int)

The report also aligns with broader international child protection and online safety principles, including:

- United Nations Convention on the Rights of the Child (UNCRC)
- WeProtect Global Alliance principles
- African Union child protection and digital rights frameworks
- International best practices on safeguarding, privacy, and survivor-centered reporting

These frameworks collectively emphasize:

- Protection of privacy and personal data
- Prevention of online exploitation and abuse
- Protection of vulnerable individuals online
- Ethical handling of digital evidence and sensitive information
- Strengthened institutional response to cyber-enabled harms

This report does not constitute legal advice and is intended primarily for awareness, prevention, policy engagement, and digital safety advocacy purposes.



Methodology

6.0 Methodology

Data was collected from the following reporting channels:

- Hotline short code (267 – MTN only)
- Dedicated call line (0545957408)
- WhatsApp messaging
- Social media platforms

Cases were reviewed and classified based on sextortion-related criteria and available information voluntarily provided by victims or complainants.

Data points reviewed included:

- Age range
- Gender
- Platform involved
- Nature of threats
- Financial demands
- Reported emotional impact
- Reporting channel used

The report uses descriptive analysis based on recorded incidents.

The analysis primarily focused on identifying recurring patterns, commonly used perpetrator tactics, platform usage trends, and operational issues affecting reporting systems. Cases were grouped according to the nature of the reported threats and available contextual information.

Where possible, incidents were reviewed to identify:

- Methods used by perpetrators
- Relationship dynamics between victims and perpetrators
- Types of extortion demands
- Technology or platforms involved
- Psychological and emotional impacts
- Emerging digital safety concerns

The report was prepared using only information directly received through the Foundation's reporting channels during the reporting period. No independent verification, forensic analysis, or criminal investigation findings were conducted by GISF for purposes of this report unless explicitly stated.



The report adopts a monitoring and trend-analysis approach rather than a prevalence or epidemiological study design. As a result, the findings should be interpreted as indicative patterns observed within reported cases and not as a comprehensive representation of all sextortion incidents occurring nationally.

To minimize risks to victims, all publicly shared case summaries were anonymized and edited to remove direct identifiers.





Ethical Reporting and Data Protection Statement

7.0 Ethical Reporting and Data Protection Statement

The Ghana Internet Safety Foundation recognizes the sensitive nature of sextortion-related incidents and the potential risks associated with disclosure.

This report has been prepared using anonymized case information. Personal identifying information including names, contact details, and other direct identifiers have been excluded from this public version.

The report aims to:

- Protect the dignity and safety of victims
- Avoid victim-blaming narratives
- Minimize risks of re-identification
- Promote ethical and trauma-informed reporting practices

The report does not disclose explicit content, images, or personally identifiable information.

The information contained in this report should not be used to harass, shame, or target victims.



Data Overview

8.0 Data Overview

A total of 120 online harm and sextortion-related cases were formally documented and validated through GISF reporting channels during the reporting period.

The relatively low number of documented cases should not be interpreted as reflecting the true scale of sextortion incidents occurring within the broader population. Available evidence from global and regional online safety studies suggests that sextortion and image-based abuse remain significantly underreported due to stigma, fear, shame, reputational concerns, and lack of confidence in reporting systems.

During the reporting period:

- January accounted for approximately 48.3% of all reported cases
- April accounted for approximately 51.7% of all reported cases
- Females represented approximately 71.7% of documented victims
- Males represented approximately 28.3% of documented victims
- Individuals aged 18–25 represented approximately 46% of all documented cases
- Child Online Protection-related cases represented approximately 40% of all documented incidents
- WhatsApp was linked to the majority of incidents, accounting for approximately 58% of reported cases
- 100% of validated reports were received through the dedicated reporting line

Additional observations included:

- Multiple cases involved emotional manipulation through fake relationships
- Financial extortion demands ranged from GHC 400 to GHC 5,000
- Several incidents involved secret recording of intimate video interactions
- Some incidents involved unauthorized access to devices or accounts
- Victims frequently reported fear, emotional distress, anxiety, and reputational concerns

The data demonstrates the growing convergence between social media usage, digital relationships, emotional manipulation, and cyber-enabled exploitation.

The findings also suggest that sextortion-related abuse in Ghana may extend beyond the currently documented figures due to reporting barriers and limited public awareness.

Monthly Case Distribution

9.0 Monthly Case Distribution

Month	Cases	Percentage
January	58	48.3%
February	0	0%
March	0	0%
April	62	51.7%
Total	120	100%

The clustering of reported cases in February and March may indicate fluctuating awareness and reporting behavior rather than an absence of incidents in other months.



Gender Distribution

10.0 Gender Distribution

Gender	Cases	Percentage
Male	86	71.7%
Female	34	28.3%
Total	120	100%

The findings indicate that female victims were disproportionately affected during the reporting period. However, the data also demonstrates that males remain vulnerable to sextortion-related exploitation.



The background features a stylized tree with a dark blue trunk and branches. The canopy is composed of several light blue circles, each containing a white silhouette of a person. The entire scene is set against a dark blue background with a subtle wood-grain texture. At the bottom center, there is a dark blue rectangular shape with a vertical slot, resembling a book or a folder. In the bottom left corner, a portion of a rainbow is visible.

Age Distribution

11.0 Age Distribution

Age Range	Cases	Percentage
10–14	18	15%
15–18	30	25%
18–25	55	46%
26–45	13	10.8%
46–64	4	3.2%
Total	120	100%

The data indicates that the majority of victims fall within the 18–25 age group, suggesting increased vulnerability among younger adults who actively use social media and messaging platforms.



Platforms Used

12.0 Platforms Used

Platform	Cases	Percentage
WhatsApp	63	52.5%
Snapchat	18	15%
Facebook	14	11.7%
TikTok	17	14.2%
Telegram	8	6.6%
Total	120	100%

WhatsApp emerged as the dominant platform linked to reported incidents, followed by Snapchat, Facebook, and TikTok.

The findings reinforce concerns regarding the misuse of messaging applications, video calls, and social networking platforms in facilitating sextortion-related abuse.



Case Classification and Emerging Trends

13.0 Case Classification and Emerging Trends

The reported cases generally fell within the following categories:

- Romance-related sextortion
- Financial sextortion
- Recorded intimate video call exploitation
- Image-based abuse
- Cyberstalking and harassment
- Account compromise and unauthorized access
- Device privacy breach incidents
- Threat-based emotional coercion

Several cases involved overlapping forms of abuse.

Table: Types of Online Harms Reported

Type of Online Harm	Description	Number of Cases	Percentage of Cases
Financial Sextortion	Monetary demands linked to threats of exposure	44	36.7%
Recorded Intimate Video Exploitation	Secret recording or misuse of intimate video calls	61	50.8%
Romance Scam / Emotional Manipulation	Use of fake identities or emotional trust to manipulate victims	49	40.8%
Threats to Leak Intimate Content	Threats to publicly release images or videos	88	73.3%
Cyberstalking / Harassment	Persistent intimidation or harassment online	31	25.8%
Account Compromise	Unauthorized access to accounts or devices	24	20%
Device Privacy Breach	Unauthorized copying or extraction of private content from devices	11	9.2%

Note: Some cases involved multiple forms of online harm simultaneously; therefore, totals exceed 100%.

Emerging trends observed during the reporting period included:

- Increased use of fake romantic identities
- Covert recording of intimate video calls
- Use of messaging platforms for extortion demands
- Financial demands ranging from GHC 400 to GHC 5,000
- Emotional manipulation and intimidation
- Use of hacked or compromised accounts
- Greater use of encrypted messaging applications
- Increased targeting of emotionally vulnerable individuals

The findings suggest that perpetrators are increasingly combining emotional manipulation, privacy violations, and financial extortion within the same abuse cycle.

The cases further demonstrate how online harms frequently overlap across categories, making it difficult to isolate incidents into a single type of abuse.



January Case Insights

14.0 January Case Insights

Cases reviewed during the reporting period revealed several recurring patterns:

- Victims were primarily young adults between 18–25 years
- Most victims were female
- Platforms involved included WhatsApp, Snapchat, Facebook, TikTok, and Telegram
- Cases often involved fake identities and manipulated trust

Common tactics used by perpetrators included:

- Fake romantic relationships
- Recorded video calls without consent
- Threats to publicly release intimate content
- Emotional manipulation and intimidation
- Financial blackmail and extortion

Reported impacts on victims included:

- Psychological trauma
- Fear and anxiety
- Social stigma
- Emotional distress
- Suicidal thoughts in some reported cases





April Case Insights

15.0 April Case Insights

Reported cases continued to reveal evolving sextortion tactics and abuse patterns.

Key observations included:

- Victims were mostly young adults aged 18–25
- One victim was in the 46–64 age range, demonstrating that older adults can also be targeted
- WhatsApp remained the dominant platform
- Cases increasingly involved unauthorized access to accounts and devices

Common tactics included:

- Secret recording of intimate interactions
- Fake online relationships
- Hacking and account compromise
- Theft or copying of private content from mobile devices
- Financial extortion demands

Reported impacts included:

- Panic and anxiety
- Financial pressure
- Emotional intimidation
- Harassment and fear of exposure
- Reputational concerns

The March cases demonstrate increasing diversification in sextortion tactics, extending beyond traditional romance scams into account compromise and device-related privacy breaches.



Perpetrator Tactics and Modus Operandi

16.0 Perpetrator Tactics and Modus Operandi

Analysis of the reported cases revealed several recurring perpetrator tactics:

- **Fake Identities and Romance Manipulation**
Perpetrators commonly posed as romantic interests to gain trust before coercing victims.
- **Secret Recording of Video Calls**
Several victims reported that intimate video calls were recorded without consent.
- **Financial Blackmail**
Perpetrators demanded payments ranging from GHC 400 to GHC 5,000.
- **Account Compromise and Cyberstalking**
Some perpetrators allegedly gained unauthorized access to victims' accounts or personal devices.
- **Device Privacy Breaches**
One reported case involved alleged theft of intimate content from a damaged mobile device by a repair technician.

These tactics highlight the need for stronger digital literacy, safer online behaviors, and improved reporting and support systems.





Impact on Victims

17.0 Impact on Victims

The cases demonstrate significant emotional, psychological, reputational, and financial impacts on victims.

Reported impacts included:

- Fear and panic
- Emotional distress
- Shame and embarrassment
- Anxiety and psychological trauma
- Financial pressure
- Social stigma
- Reluctance to report incidents
- Suicidal thoughts in extreme cases

Several victims described experiences consistent with emotional intimidation, prolonged anxiety, fear of exposure, and reputational concerns. Victims often expressed fear that intimate material could be circulated publicly among family members, friends, schools, workplaces, or social media communities.

The emotional consequences of sextortion can extend beyond the immediate incident. Victims may experience:

- Loss of trust in online relationships
- Withdrawal from social interactions
- Academic or workplace disruptions
- Persistent fear of future harassment
- Long-term psychological distress

The findings also suggest that shame and stigma remain major barriers to reporting. Many victims of sextortion may choose not to seek help due to fear of judgment, victim-blaming, or reputational damage.

The report further highlights the growing need for trauma-informed response systems capable of providing emotional support, safety planning, referral pathways, and guidance to victims navigating online abuse situations.

The findings reinforce the importance of integrating mental health and psychosocial support into online safety response systems.



Reporting Channels Analysis

18.0 Reporting Channels Analysis

Reporting Channel	Cases	Percentage
GISF Hotline 267	0	0%
Other GISF Reporting Channels	100	0%

The dedicated call line functioned as the primary and only effective reporting mechanism during the reporting period.

The GISF Hotline 267 system experienced significant operational challenges, including:

- Accidental calls
- Wrong-number inquiries
- Unrelated requests
- Misidentification of the hotline purpose

The findings indicate a need for improved public education and hotline optimization.



National CyberTip and Hotline-Linked Trends in Ghana (Ghana Police Service)

National CyberTip and Hotline-Linked Trends in Ghana (Ghana Police Service)

Available national-level reporting statistics referenced through CyberTip and hotline-linked reporting mechanisms in Ghana further reinforce the growing scale and complexity of online child protection concerns.

According to publicly referenced CyberTip-related reporting data highlighted in national media discussions in Ghana between January 2025 and June 2025, significant volumes of online child exploitation-related material and incidents were identified through reporting systems and law enforcement-linked mechanisms.

File Information Uploaded Through Reporting Platforms

Type of File Uploaded	Reported Volume
Child Sexual Abuse Material generated using AI	Less than 50 files
Images	Approximately 11,000 files
Videos	Approximately 35,000 files
Other Files (ZIP, PDF, etc.)	Approximately 8,700 files

The volume of reported videos significantly exceeded image-based reports, highlighting the growing circulation and sharing of video-based exploitative content online.

The presence of AI-generated child sexual abuse material, although reported at relatively lower volumes, demonstrates the emerging risks associated with generative artificial intelligence technologies and their potential misuse in child exploitation ecosystems.

The large number of uploaded compressed files and document-based submissions further suggests increasing sophistication in how exploitative material is packaged, transferred, concealed, and distributed across digital platforms.



Reported Incident Categories Linked to CyberTip Reporting Data (Jan 2025 – June 2025)

Type of Incident	Number of Reported Cases
Child Pornography (Possession and Distribution)	18,000
Child Sexual Molestation	Less than 50
Child Sex Tourism	Less than 50
Child Sex Trafficking	100
Misleading Domain Name	Less than 50
Misleading Words / Images	Less than 50
Online Enticement	800
Unsolicited Obscene Material	100

These statistics provide important national context for understanding the broader online child protection environment in Ghana.

The extremely high volume of reported child sexual abuse material (CSAM) cases linked to possession and distribution highlights the seriousness of online exploitation risks and demonstrates the increasing role of digital platforms in facilitating harmful content circulation.

The reported online enticement cases also reinforce growing concerns regarding online grooming, manipulation, and exploitation of children through social media, messaging applications, gaming environments, and other online communication channels.

The relatively lower figures recorded under child sexual molestation and child sex tourism should not necessarily be interpreted as low prevalence. Such incidents are frequently underreported due to stigma, fear, family pressure, lack of awareness, and challenges associated with evidence collection and reporting.



The data further demonstrates that online harms affecting children increasingly extend beyond traditional sextortion cases and now involve a wider ecosystem of online grooming, exploitation, coercion, trafficking risks, exposure to obscene materials, and digital manipulation.

For GISF, these national-level trends reinforce the importance of:

- Strengthening Child Online Protection interventions
- Expanding awareness campaigns targeting schools and parents
- Improving digital literacy among children and adolescents
- Strengthening collaboration with law enforcement and national response systems
- Supporting safer reporting pathways for children and vulnerable individuals
- Promoting early intervention and psychosocial support systems

The findings also reinforce the growing need for multi-stakeholder collaboration involving civil society organizations, schools, telecommunications providers, technology platforms, parents, mental health professionals, and law enforcement agencies.

While the GISF dataset in this report reflects cases directly reported through Foundation-linked reporting mechanisms, the broader CyberTip-related statistics demonstrate that online child exploitation and abuse concerns in Ghana may be substantially larger than currently reflected within civil society reporting channels alone.



Key Observations

19.0 Key Observations

1. GISF Hotline 267 Continues to Serve as an Important Reporting Channel

The reporting period demonstrates that the GISF Hotline 267 remains an important access point for individuals seeking support and guidance regarding online harms and sextortion-related incidents.

The findings suggest the need for continued public education to improve understanding of the hotline's purpose and encourage more accurate and timely reporting of online safety concerns.

The reporting trends also demonstrate growing public awareness regarding GISF's role in online safety and child protection advocacy.

2. Reporting Patterns Reflect Awareness and Visibility

The concentration of reports in January and April suggests that awareness and accessibility may significantly influence reporting behavior.

3. Social Media and Messaging Platforms Remain Primary Risk Areas

A significant proportion of reported incidents were linked to social media and messaging platforms including WhatsApp, Snapchat, Facebook, TikTok, Telegram, and video-calling environments.

WhatsApp emerged as the most frequently referenced platform within reported cases, particularly in incidents involving:

- Recorded intimate video calls
- Financial sextortion demands
- Emotional manipulation
- Threats to release intimate content
- Blackmail and coercion



Snapchat and TikTok-related cases were more commonly associated with:

- Youth interactions
- Temporary or disappearing content features
- Online grooming indicators
- Peer-related exploitation and harassment

Facebook-linked incidents frequently involved:

- Fake identities
- Romance scam-related manipulation
- Impersonation
- Migration of conversations from public platforms to encrypted messaging applications

Telegram-related reports, although fewer in number, reflected concerns regarding privacy-focused environments that may enable anonymous communication and harmful content sharing.

The findings reinforce the growing role of digital communication platforms in facilitating emotional manipulation, coercion, cyberstalking, grooming, and sextortion-related abuse.

4. Young Adults Remain Highly Vulnerable

The overwhelming majority of victims fell within the 18–25 age group.

5. Emotional and Psychological Harm is Significant

Victims frequently reported fear, shame, distress, and emotional trauma.

6. Financial Sextortion is Increasingly Evident

Several cases involved direct monetary extortion demands.

Key Observations and Challenges

20.0 Key Observations and Challenges

The reporting period revealed several important trends regarding online harms, sextortion, and Child Online Protection concerns in Ghana.

The findings demonstrate that social media and messaging applications continue to serve as primary environments through which online exploitation, emotional manipulation, blackmail, and cyber-enabled abuse occur. WhatsApp remained the most frequently referenced platform within reported cases, particularly in incidents involving recorded intimate video interactions, threats to release private content, financial extortion, and emotional coercion.

Snapchat and TikTok-related incidents were more frequently associated with younger users, including students and adolescents. These platforms were linked to concerns involving disappearing content, peer exploitation, online grooming indicators, cyberbullying, and image-sharing behaviors.

Facebook-linked incidents commonly involved fake identities, impersonation, romance scam-related manipulation, and migration of conversations toward more private or encrypted communication environments.

The report also demonstrates the growing vulnerability of children, adolescents, and young adults to online harms. A significant proportion of reported incidents involved Child Online Protection-related concerns affecting school-aged victims, particularly within the Senior High School age bracket.

Emotionally manipulative tactics remained common across many reported cases. Victims frequently described experiences involving fear, shame, anxiety, reputational concerns, and prolonged emotional distress. Several cases reflected indicators of psychological trauma and social withdrawal.

The reporting period further highlighted ongoing operational challenges associated with online safety response work, including underreporting, stigma, evolving perpetrator tactics, limited awareness regarding reporting pathways, and the emotional sensitivity surrounding online exploitation cases.

Despite these challenges, the findings also suggest growing public awareness regarding GISF's reporting and awareness initiatives. The increasing use of reporting channels demonstrates rising public willingness to seek support regarding online harms and sextortion-related abuse.

Safeguarding and Survivor Protection Considerations

21.0 Safeguarding and Survivor Protection Considerations

The Ghana Internet Safety Foundation recognizes the need for survivor-centered and trauma-informed approaches when handling sextortion-related reports.

Several cases involved serious emotional distress, including indications of trauma and suicidal thoughts.

The Foundation therefore recognizes the importance of:

- Confidential handling of reports
- Survivor dignity and privacy protection
- Safe referrals to mental health professionals where necessary
- Strengthened collaboration with law enforcement and victim support stakeholders
- Clear escalation pathways for high-risk cases

This report does not claim that formal clinical or legal interventions were provided in every case. However, the findings reinforce the need for stronger safeguarding systems and coordinated response mechanisms.



Evidence Preservation and Incident Response Guidance

22.0 Evidence Preservation and Incident Response Guidance

Victims of sextortion are encouraged to preserve available evidence where safe to do so.

Relevant evidence may include:

- Screenshots
- Phone numbers
- Usernames and account IDs
- Payment requests
- Chat records
- URLs and social media profiles
- Threat messages

Victims are generally encouraged not to delete evidence immediately, as it may support investigations or platform reporting.

Where appropriate, victims should also consider:

- Reporting compromised accounts
- Changing passwords
- Enabling multi-factor authentication
- Reporting abusive accounts to platforms
- Seeking support from trusted institutions or professionals



Recommendations and Future Priorities

23.0 Recommendations and Future Priorities

The findings from the reporting period demonstrate the urgent need for sustained investment in prevention, awareness creation, safeguarding systems, and survivor-centered support mechanisms.

Public awareness campaigns remain critical, particularly among young people, students, parents, and educators. The report demonstrates that many online harm incidents continue to originate through social media interactions, emotional manipulation, and unsafe digital engagement practices. Future awareness initiatives should therefore focus not only on sextortion itself, but also on broader digital literacy, privacy protection, online grooming awareness, and responsible online behavior.

The findings also reinforce the importance of strengthening collaboration between civil society organizations, schools, law enforcement agencies, mental health professionals, telecommunications providers, and technology platforms. Online harms increasingly operate across multiple digital environments, making coordinated response mechanisms essential.

The GISF Hotline 267 continues to serve as an important reporting and support mechanism for victims of online harms. Continued public education is needed to ensure individuals understand how and when to use the hotline effectively. Increased visibility of reporting channels may also encourage earlier reporting and reduce the emotional and psychological escalation often associated with prolonged online abuse.

The report further highlights the growing importance of Child Online Protection interventions within Ghana. The significant proportion of reported incidents involving children and adolescents demonstrates the need for stronger school-based awareness campaigns, digital parenting support, and youth-centered online safety education.

Future interventions should also prioritize:

- Improved digital literacy and cyber hygiene
- Stronger psychosocial and safeguarding support pathways
- Better documentation and data collection practices
- Increased public trust in reporting systems
- Early intervention mechanisms for children and vulnerable individuals
- Continued stakeholder engagement on online safety and child protection issues

As online harms continue to evolve alongside digital technologies, future response efforts must remain adaptive, collaborative, and survivor-centered.



Conclusion

24.0 Conclusion

Future monitoring efforts should seek to improve:

- Reporting consistency
- Hotline performance metrics
- Victim referral tracking
- Awareness campaign reach
- Response timelines
- Data quality and classification standards

The Foundation also recognizes the need for more longitudinal data to better understand national sextortion trends over time.



Limitations of the Report

25.0 Limitations of the Report

This report has several limitations:

- The data reflects only reported cases received through GISF channels
- Sextortion remains significantly underreported
- Some case details were incomplete
- Reporting patterns may be influenced by awareness campaigns and visibility
- The report does not represent national prevalence
- Some victims may have reported incidents through other institutions or not reported at all

The findings should therefore be interpreted cautiously.



Conclusion

26.0 Conclusion

The combined analysis demonstrates that sextortion remains a serious but underreported online safety concern.

While 120 cases were documented during the reporting period, the findings reveal broader concerns regarding online exploitation, digital privacy abuse, emotional coercion, and financial blackmail.

The report highlights the increasing misuse of messaging and social networking platforms, the vulnerability of young adults, and the emotional and psychological impact of sextortion-related abuse.

The complete reliance on the dedicated call line and the operational weaknesses of the hotline system further demonstrate important gaps in reporting infrastructure.

Addressing sextortion effectively will require:

- Stronger awareness initiatives
- Improved reporting systems
- Better safeguarding mechanisms
- Survivor-centered support systems
- Enhanced collaboration among stakeholders
- Increased public trust and engagement

The Ghana Internet Safety Foundation remains committed to supporting safer online environments, strengthening digital literacy, and improving awareness and response efforts relating to online harms.



Appendix – Anonymized Case Summaries

27.0 Appendix - Anonymized Case Summaries

January Case Summaries

Case 1

An 18-year-old female victim reported harassment following the circulation of an intimate video allegedly recorded without her consent during intercourse with her boyfriend. The incident reportedly resulted in prolonged emotional trauma and withdrawal from school.

Case 2

An 18-year-old male victim reported being deceived by an individual posing as a woman on Facebook. The interaction moved to WhatsApp where an intimate video call was allegedly recorded and used for blackmail.

Case 3

A 21-year-old female victim reported threats involving private images allegedly accessed by an individual online.

Case 4

A 20-year-old female victim reported receiving threats relating to intimate videos allegedly shared previously with another individual.

Case 5

A 25-year-old female victim reported threats from a romantic partner involving the release of intimate photographs.

Case 6

A 23-year-old female victim reported participating in an intimate video call that was allegedly recorded and later used for blackmail and intimidation.

April Case Summaries

Case 1

A 19-year-old female victim reported that an intimate video call was recorded without consent and later used to threaten public exposure.

Case 2

A 48-year-old female victim reported prolonged harassment and alleged unauthorized access to her phone number and TikTok account by a former partner.

Case 3

A 19-year-old female victim reported that intimate content was allegedly copied from a damaged mobile device and later used for blackmail.

Case 4

A 22-year-old male victim reported being secretly recorded during an intimate video call and later extorted for money.

Case 5

A 20-year-old female victim reported receiving threats from an individual claiming to possess intimate images.

Case 6

A 20-year-old female victim reported receiving financial extortion demands relating to a recorded intimate video call.

