2025 SEXTORTION REPORT

DIGITAL FORENSICS CORP

TABLE OF CONTENTS

FOREWORD

At Digital Forensics Corp., our mission is to provide clients with exceptional cybersecurity solutions and expert guidance to navigate the complexities of cybercrime. Every case we handle and every resource we share is backed by our team of licensed private investigators, certified forensic examiners, and ethical hackers, who bring extensive knowledge of digital threats, security protocols, and forensic methodologies.

This report is designed to equip victims, law enforcement, and the public with critical insights into this growing issue. It offers seasoned expertise and proactive strategies to combat today's most prevalent sextortion threats. Utilizing court-approved forensic applications and software, our team ensures precise and legally sound digital investigations that stand up to scrutiny.

We take pride in upholding the highest standards of professionalism, ethics, and confidentiality, ensuring that our clients feel secure and supported every step of the way.

Sean Quellos

Senior Forensic Engineer

Digital Forensics Corp.

At Digital Forensics Corp., we have long been at the forefront of cybersecurity, helping individuals and organizations safeguard their digital lives against cyber threats. However, in recent years, one crime has risen at an alarming rate...sextortion.

As a cybersecurity firm, we first encountered sextortion through distressed clients seeking help in reclaiming control over their digital presence. This form of online blackmail, where perpetrators manipulate victims into paying money in exchange for silence, has become a growing epidemic with devastating financial and emotional consequences.

Recognizing the scale of the issue, we expanded our services to provide remediation and support for victims, helping them mitigate the damage and seek justice.

This report is based on a small collection of processed cases from December 2024 through January 2025. It aims to demystify sextortion by breaking down real-world data. This includes who is being targeted, cyber criminals' chosen platforms, and the financial toll victims face. Our analysis of nearly 1,000 sextortion cases revealed some troubling trends.

While the numbers are staggering, there is a way forward. If you or someone you know is a victim of sextortion, **DO NOT PAY YOUR BLACKMAILER**. These crimes thrive on secrecy, and compliance only encourages further exploitation. Instead, the incident should be reported to local law enforcement agencies specializing in cybercrime. Digital evidence can be traced, and intervention is possible.

At Digital Forensics Corp., we remain committed to combating this cybercrime by providing victims with the tools and support to reclaim control. We hope this report serves as both a warning and a resource in the fight against sextortion.

RESOURCES FOR VICTIMS

Sextortion impacts people of all ages. If you or someone you love is targeted, please seek help from the following organizations.

Resources for Adults:

FBI Internet Crime Complaint Center (IC3) ic3.gov or call 1-800-CALL-FBI

Resources for Minors:

National Center for Missing & Exploited Children https://report.cybertip.org/

EXECUTIVE SUMMARY

Sextortion has rapidly evolved into one of the most prevalent and financially devastating forms of cybercrime. As a leading cybersecurity firm, Digital Forensics Corp. has worked closely with victims seeking remediation, uncovering alarming patterns in how these crimes occur, who is being targeted, and the scale of financial loss.

This report, based on 942 cases analyzed over two months, provides critical insights into the mechanics of sextortion, shedding light on the platforms exploited, the demographic groups most at risk, and the tactics used by perpetrators.

TAKEAWAYS

Sextortion thrives on secrecy and fear. Many victims comply out of desperation, believing that paying will stop the threats, but compliance often leads to repeated demands.

If you or someone you know is being targeted:

1. Do not pay your blackmailer. Paying only encourages further exploitation.
2. Document all communications (screenshots, emails, messages) as potential evidence.
3. Report the crime immediately to law enforcement agencies that specialize in cybercrime.
4. Seek professional cybersecurity assistance to secure your digital accounts and prevent further breaches.

*Values based on a sample dataset of 942 cases collected between December 2024 and January 2025, providing a focused analysis of emerging sextortion threats within this period.

KEY FINDINGS

98.83%

Of processed cases involved perpetrators demanding money in exchange for not leaking the victim's content.

62%

Of victims complied with their blackmailer's initial demands., emboldening criminals and fueling repeat threats.

98%

Of victims never reported the crime to law enforcement, with even less reporting to platform administrators, allowing perpetrators to continue exploiting others

THE VICTIMS

Sextortion is often misunderstood. Many assume that victims are primarily women or minors, or that only those who engage in risky online behavior are at risk. Instead, it is an indiscriminate crime that can target anyone, regardless of gender, age, or background. The perpetrators behind these schemes do not select victims based on reckless behavior. They exploit social engineering techniques to trick victims into sending their intimate content.

WHO IS MOST AT RISK

Sextortion does not discriminate—it affects people of all ages, backgrounds, and digital habits. However, our data reveals a stark divide between younger and older victims. **Those under 40 make up 59.32% of cases, while those 40 and older account for 40.68%.This trend suggests that younger adults are at the highest risk**, likely due to their active presence on dating apps, social media, and messaging platforms. Meanwhile, older victims may be targeted through scams that exploit financial stability and professional reputations.

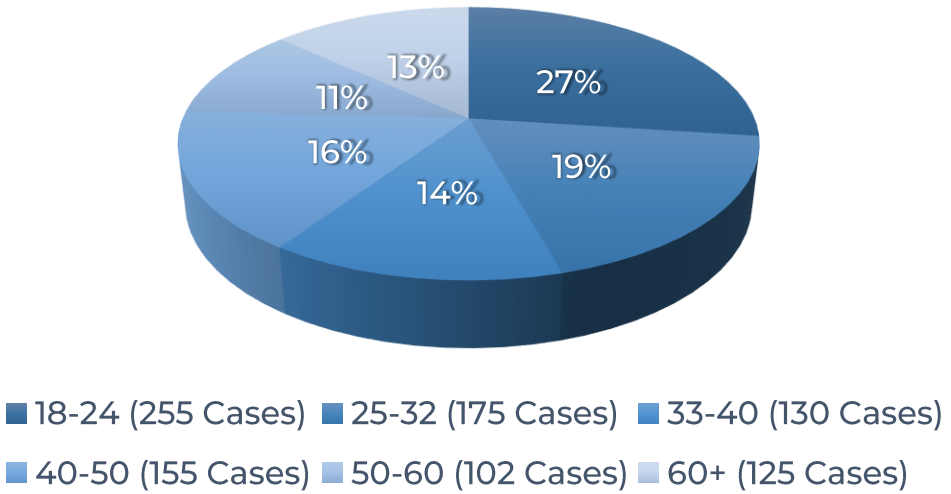
Younger victims were heavily represented in our study of sextortion cases, with the **highest percentage of victims falling between 18-24 years old**. These individuals are more likely to engage in online interactions, including dating apps, casual social media exchanges, and private messaging platforms. Many may also lack awareness of the tactics used by scammers, making them more vulnerable.

While older adults were less frequently targeted than their younger counterparts, older victims still represent a significant share of cases. Many in this category are approached under the guise of professional or romantic interest, particularly through platforms like Facebook, LinkedIn, or encrypted messaging apps. Scammers may use long-term grooming tactics, building trust before initiating tactics to gain intimate content and blackmail their victims.

Age Breakdown: Under 40 vs. Over 40

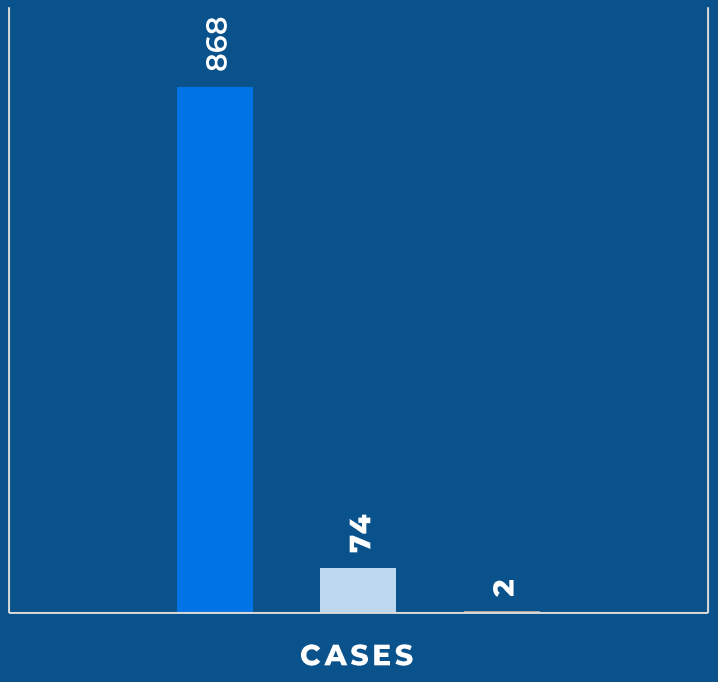
- Victims Under 40 (59.32% / 560 Cases)
- Victims Over 40 (40.68% / 384 Cases)

SEXTORTION CASES BASED ON AGE



*Values based on a sample dataset of 942 cases collected between December 2024 and January 2025, providing a focused analysis of emerging sextortion threats within this period.

VICTIMS BY GENDER



GENDER OF TARGETS

Based on responses from those surveyed, sextortion overwhelmingly targeted men, a fact that contradicts the common belief that online exploitation primarily affects women.

While women are often thought to be at greater risk in terms of image based sexual abuse, this data reveals that men, particularly young men, are the most frequent targets of financial sextortion.

Understanding who is most at risk is only part of the picture, equally important is recognizing how these schemes unfold. The next section delves into the tactics used by perpetrators, exploring how they initiate contact, build trust, and ultimately manipulate victims into compliance.

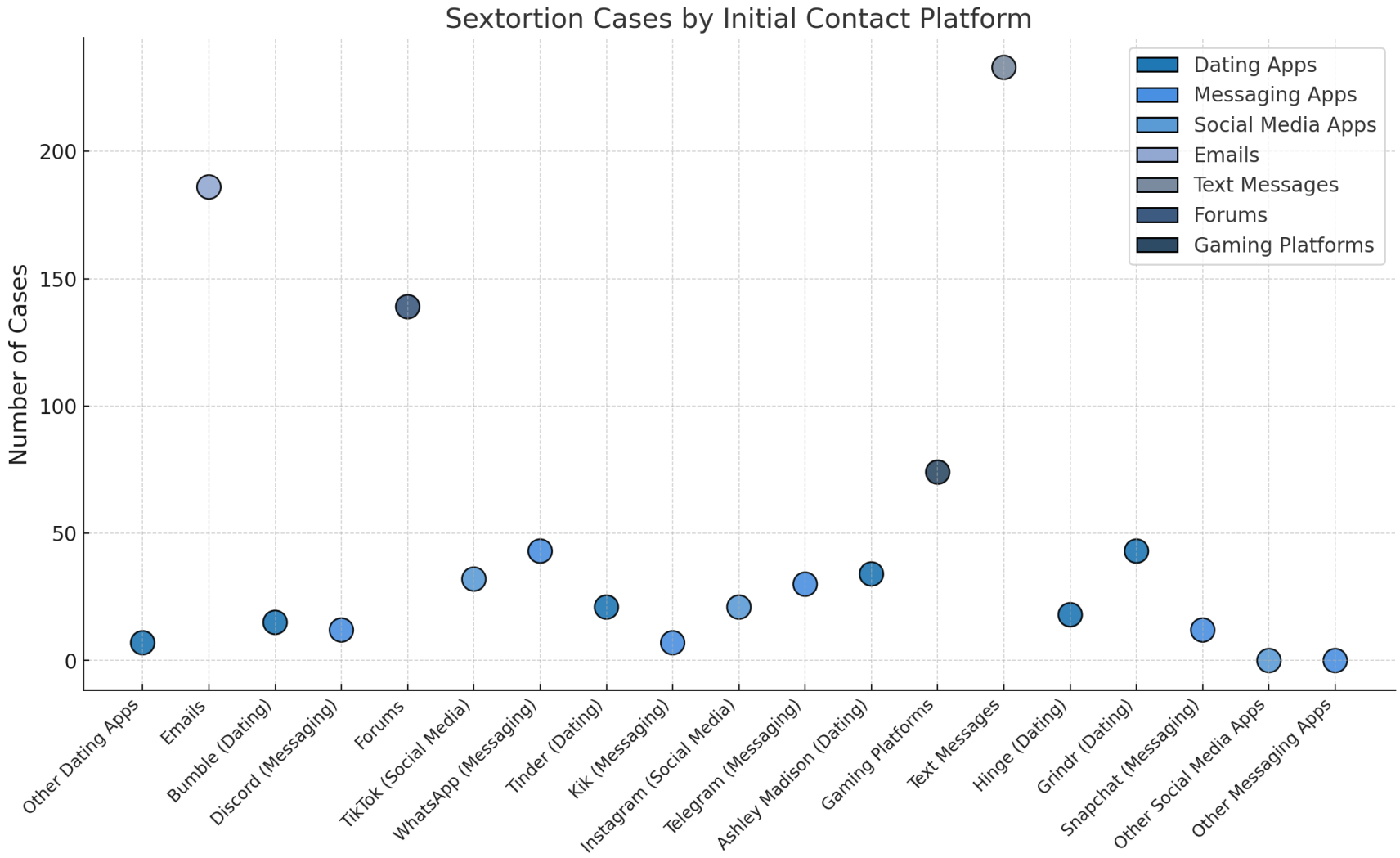
WHERE IT BEGINS

Sextortion schemes do not happen by chance, they start with carefully planned interactions on specific digital platforms. The data in this report shows that sextortion cases originate in a variety of different digital platforms including social media, messaging apps, and dating platforms. While these services were designed to foster connection, scammers have weaponized them.

Our analysis of 933 cases of those surveyed reveals the following about applications where cybercriminals hunt for new targets.

PLATFORMS USED BY SCAMMERS

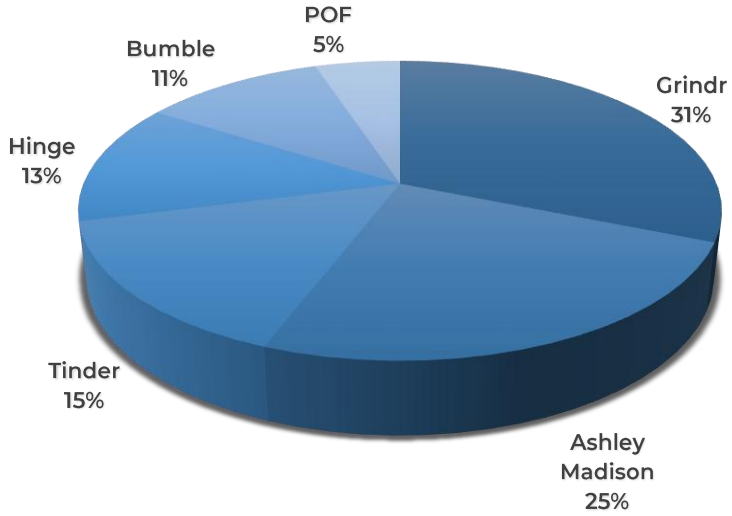
Sextortion schemes span multiple digital platforms, with **14.79% of cases starting on dating apps**, where scammers exploit intimacy**. Messaging apps account for 11.15%,** providing direct access to victims, while social media (5.68%) enables fraud through fake personas. The largest share **(68.38%) comes from emails, text messages, job fraud, and gaming platforms**, proving sextortion is not confined to a single space, scammers strike wherever they can gain control.



*Values based on a sample dataset of 942 cases collected between December 2024 and January 2025, providing a focused analysis of emerging sextortion threats within this period.

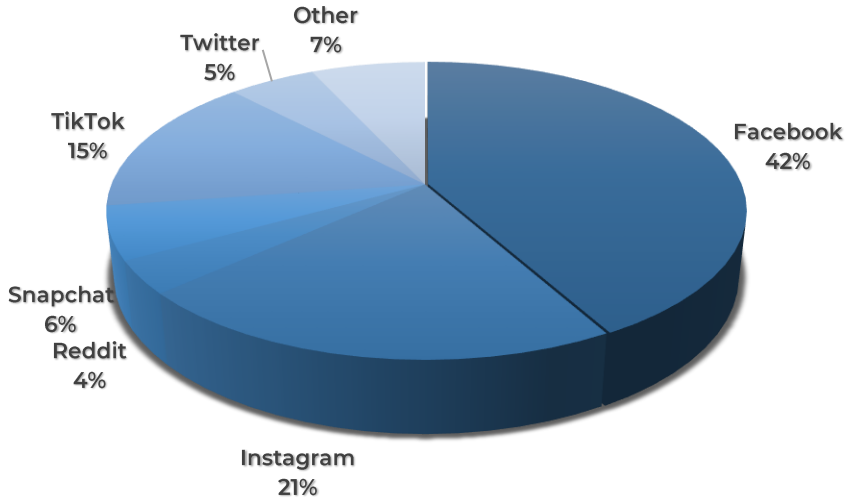
DATING APPLICATIONS

Dating apps are a major target for sextortion, with scammers exploiting intimacy to gain leverage. Grindr (31%) and Ashley Madison (25%) lead in cases, followed by Tinder, Hinge, and Bumble. Scammers build trust quickly, then coerce victims, often urging them to switch to encrypted apps. Users should stay alert for rushed intimacy and suspicious requests.



SOCIAL MEDIA APPLICATIONS

Social media platforms play a key role in sextortion, with scammers posing as influencers or attractive strangers to lure victims. Facebook (42%) and Instagram (21%) account for most cases, where direct messaging enables rapid exploitation. Users should be wary of unsolicited messages, sudden escalations in intimacy, and requests to move conversations to private messaging apps, common tactics used in sextortion schemes.



*Values based on a sample dataset of 942 cases collected between December 2024 and January 2025, providing a focused analysis of emerging sextortion threats within this period.

THE IMPACT

Sextortion is not just a psychological and emotional burden; it also comes with significant financial consequences. Over **62% of victims surveyed** complied with financial demands, with reported losses ranging from under $500 to over $100,000.

FINANCIAL LOSS

The average financial loss per victim was **$2,390.60**, though scammers often escalate their demands once initial payments are made. Paying rarely stops the threats—instead, victims are frequently targeted for more money.

The Hidden Cost: Long-Term Damage

Beyond financial loss, victims experience severe emotional distress, social withdrawal, and reputational fears. Many suffer ongoing harassment, even after payment. With 98% of cases unreported, scammers continue to exploit victims without consequence.

Key Takeaway: Never Pay the Blackmailer.

Sextortion thrives on fear and secrecy, but compliance only emboldens criminals. If targeted, victims should delay payment, document threats, and report the crime immediately to law enforcement and cybersecurity professionals.

Among victims who paid the blackmailer, the frequency of threats was alarming:

- 39.59% received threats daily after complying.
- 26.11% were targeted weekly with further demands.
- 24.06% were harassed multiple times per day.

These figures highlight that paying does not stop the threats—instead, it often escalates the extortion. Scammers continue to demand more, trapping victims in a cycle of financial and psychological distress.

39.93% of victims paid under $500.

26.45% lost between $500 – $1,000.

22.70% suffered losses between $1,000 – $5,000.

5.29% paid between $5,000 – $25,000.

0.51% were extorted for $25,000 – $100,000.

0.34% lost over $100,000.

*Values and percentages based on 586 responses where the victim advised they'd paid some amount to their blackmailer.

WHO IS MOST AT RISK

Sextortion does not discriminate—it affects people of all ages, backgrounds, and digital habits. However, our data reveals a stark divide between younger and older victims. **Those under 40 make up 59.32% of cases, while those 40 and older account for 40.68%.This trend suggests that younger adults are at the highest risk**, likely due to their active presence on dating apps, social media, and messaging platforms. Meanwhile, older victims may be targeted through scams that exploit financial stability and professional reputations.

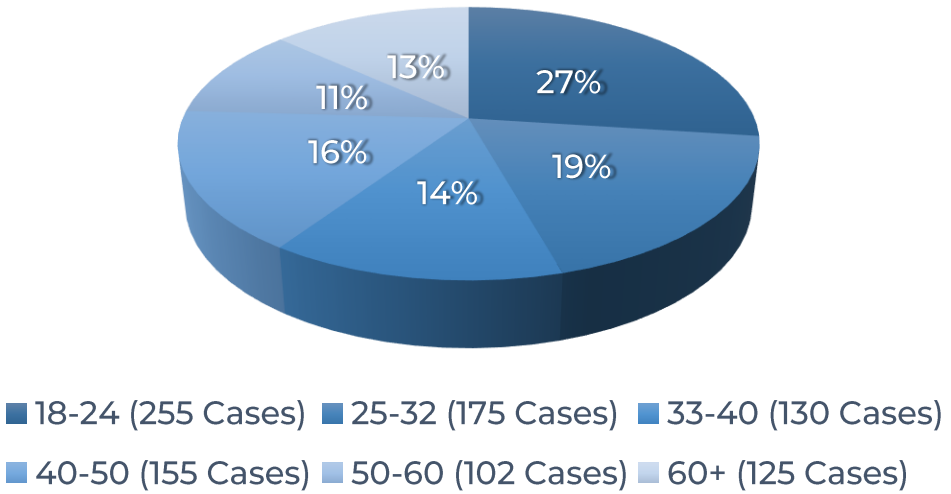
Younger victims were heavily represented in our study of sextortion cases, with the **highest percentage of victims falling between 18-24 years old**. These individuals are more likely to engage in online interactions, including dating apps, casual social media exchanges, and private messaging platforms. Many may also lack awareness of the tactics used by scammers, making them more vulnerable.

While older adults were less frequently targeted than their younger counterparts, older victims still represent a significant share of cases. Many in this category are approached under the guise of professional or romantic interest, particularly through platforms like Facebook, LinkedIn, or encrypted messaging apps. Scammers may use long-term grooming tactics, building trust before initiating tactics to gain intimate content and blackmailer their victim.

Age Breakdown: Under 40 vs. Over 40

- Victims Under 40 (59.32% / 560 Cases)
- Victims Over 40 (40.68% / 384 Cases)

SEXTORTION CASES BASED ON AGE



*Values based on a sample dataset of 942 cases collected between December 2024 and January 2025, providing a focused analysis of emerging sextortion threats within this period.

APPENDIX A: DEFINITIONS

Financial Sextortion: A form of online blackmail where a perpetrator threatens to distribute intimate images, videos, or AI generated content unless the victim complies with demands for payment in exchange for silence.

Sexploitation/Content Sextortion: A form of online blackmail where a perpetrator threatens to distribute intimate images, videos, or AI generated content unless the victim complies with demands for additional sexual content or favors from the victim.

Online Blackmail: The act of using private, sensitive, or compromising information to extort money, services or compliance form an individual

Cyber Extortion: A broader term for digital threats involving ransom demands, such as threats to expose private data, hack accounts, or release damaging material.

Revenge Porn: The non-consensual distribution of intimate images, often as an act of revenge or coercion.

Catfishing: An act of fraud where a person creates a fake online identity to trick others into relationships, scams, or financial fraud.

Deepfake: AI generated media, often used maliciously to create fake explicit images or videos of victims.

AI-Generated Sextortion Scams: A broad term used to define the use of artificial intelligence to complete one or multiple actions in a sextortion scam. This may include creation of content, voice cloning, or generative response.

Content Removal Services: Professional services that assist victims in removing non-consensual content from online platforms.

Law Enforcement Agencies for Cybercrime: Government entities such as the FBI's Internet Crime Complaint Center (IC3) in the United States or the National Cyber Security Center (NCSC) in the UK, which investigate cyber extortion cases.

APPENDIX B: ADDITIONAL INFORMATION REGARDING DATA

- Values based on a sample dataset of 942 cases collected between December 2024 and January 2025, providing a focused analysis of emerging sextortion threats within this period.
- As appropriate, cases of sextortion reported to DFC are reviewed with the type of crime adjusted based on the details of the case.
- Cases are classified as sextortion based on the threat of exposure if not compensated financially. Cases where the blackmailer requests additional content are filed as sexploitation.
- Platform of initial contact is designated as the platform where the victim believes they met and shared their content with the blackmailer.
- Platform of initial threat is designated as the platform where the victim received the first threat of exposure if not compensated.
- Losses reported in foreign currencies are converted to U.S. dollars when possible.
- No cases were filed more than once in an effort to avoid the possibility of duplicate reports.
- To maintain confidentiality and protect client identities, some data has been redacted from DFC's findings.
- DFC is committed to providing further analysis concerning sextortion and other emerging cybercrimes in future reports.

ABOUT DIGITAL FORENSICS CORP.

Digital Forensics Corp. (DFC) is a leading cybersecurity and digital forensics firm specializing in cybercrime investigation, data security, and online threat mitigation. With years of experience handling complex cyber threats, DFC has become a trusted partner for individuals, businesses, and law enforcement agencies seeking to combat digital fraud, extortion, and cyber exploitation.

If you or someone you know is facing sextortion or any other form of cybercrime, do not engage with the perpetrator. Instead, report the incident to law enforcement and seek expert guidance. DFC is here to help.

We will continue to publish information on sextortion and other emerging cybercrimes in future reports.

DISCLAIMER

All information presented by Digital Forensics Corp. is provided for educational purposes only. Any case studies, examples, or discussions do not disclose the identities of any clients or individuals. DFC maintains strict confidentiality and adheres to ethical and legal standards in all cybersecurity and investigative practices.

digitalforensics.com | Toll-Free: 800.849.6515

DIGITAL FORENSICS CORP