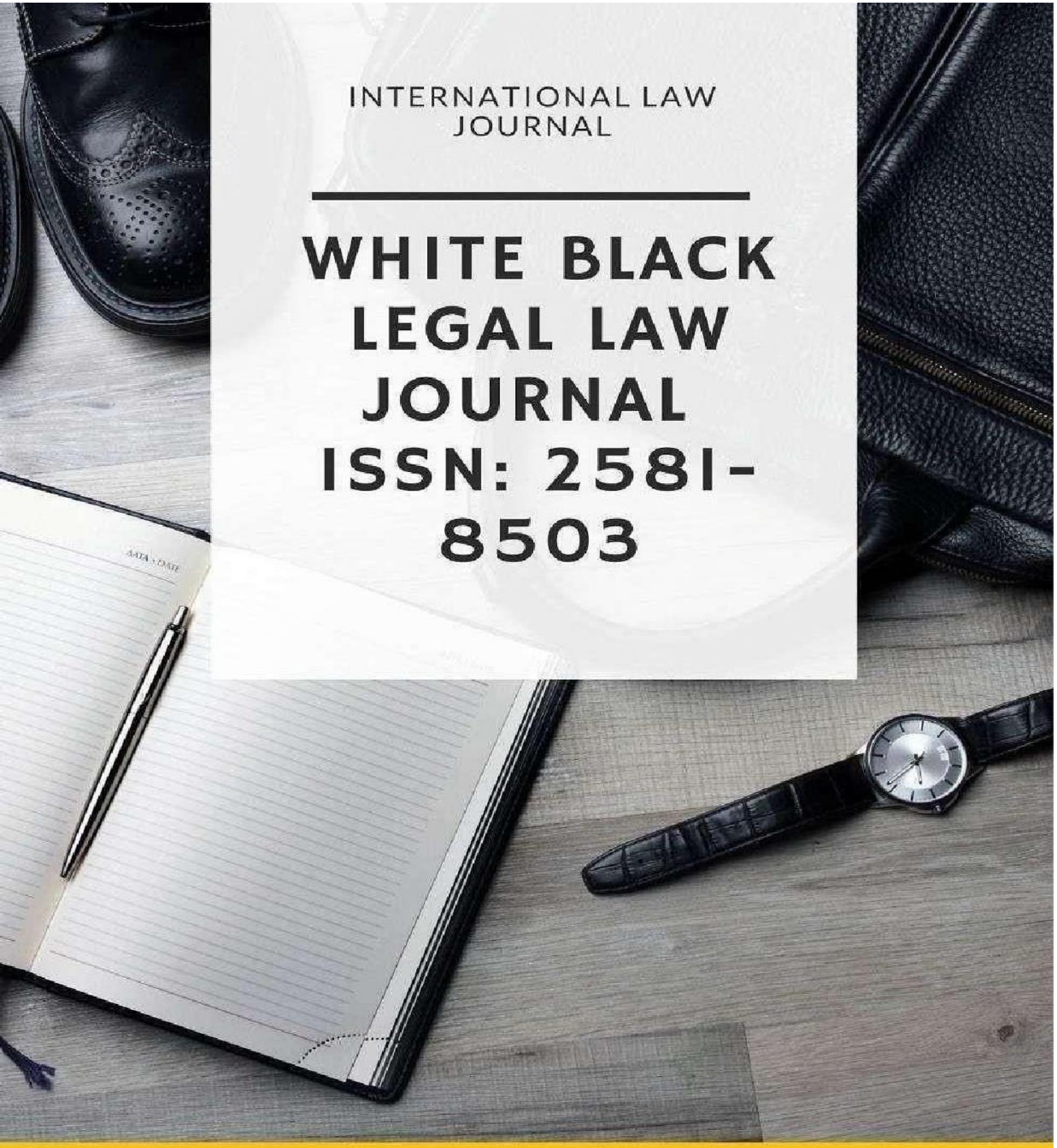


INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

The views, opinions, interpretations, and conclusions expressed in the articles are exclusively those of the respective authors. They do not represent or reflect the views of the Editorial Board, Editors, Reviewers, Advisors, Publisher, or Management of *White Black Legal*.

While reasonable efforts are made to ensure academic quality and accuracy through editorial and peer-review processes, *White Black Legal* makes no representations or warranties, express or implied, regarding the completeness, accuracy, reliability, or suitability of the content published. The journal shall not be liable for any errors, omissions, inaccuracies, or consequences arising from the use, interpretation, or reliance upon the information contained in this publication.

The content published in this journal is intended solely for academic and informational purposes and shall not be construed as legal advice, professional advice, or legal opinion. *White Black Legal* expressly disclaims all liability for any loss, damage, claim, or legal consequence arising directly or indirectly from the use of any material published herein.

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

"CYBER MALEFICATION AGAINST ON INSTAGRAM"

AUTHORED BY - K.KEERTHANA.,
BA.LLB., LLM.

TABLE OF CONTENTS

Abstract

Instagram has emerged as one of the most influential social networking platforms, connecting millions of users for communication, entertainment, business, and information sharing. However, its widespread use and large volume of personal data have also made it an attractive environment for cybercriminal activities. Users may encounter threats such as phishing, account hijacking, identity impersonation, online scams, cyber harassment, data exposure, malicious bots, deepfakes, and sextortion. This paper examines the major forms of cybercrime associated with Instagram and analyses the factors that make users vulnerable to these attacks. It considers how cybercriminals exploit human behaviour, weak security practices, social engineering techniques, and platform features to deceive victims and gain unauthorized access to accounts or personal information. The study also considers the social, psychological, financial, and reputational consequences experienced by individuals affected by Instagram-related cybercrime.

Further, the paper examines the legal and regulatory mechanisms applicable to cyber offences committed through social media platforms, with particular attention to the Indian legal framework. Selected incidents and practical examples are used to understand the changing methods adopted by cybercriminals and to assess the effectiveness of existing platform-level security measures. The study also highlights the growing importance of artificial intelligence, ethical hacking, automated threat detection, and cooperation among social media companies, law-enforcement agencies, cybersecurity professionals, and users.

The paper concludes that technological safeguards alone cannot completely prevent cybercrime on Instagram. A stronger cybersecurity environment requires a combination of user awareness, responsible platform design, effective reporting mechanisms, timely law-enforcement action, privacy protection, and continuous technological innovation. The study therefore proposes practical measures for users, Instagram, cybersecurity stakeholders, and policymakers to improve digital safety and strengthen resilience against emerging cyber threats.

Keywords: Cybercrime, Instagram, Social Media Security, Phishing, Identity Theft, Account Takeover, Deepfake, Sextortion, Malware, Online Privacy, Cybersecurity, Social Engineering

Introduction:

In today's digital age, social media platforms have become integral to communication, commerce, and community engagement. Among them, Instagram stands out as a dominant force, boasting over two billion users worldwide. With its visually driven interface and widespread appeal among individuals, influencers, brands, and businesses, Instagram has transformed how people share content, promote products, and interact globally.

However, with this popularity comes a darker reality—cybercrime. As Instagram's user base and functionalities have grown, so too has its attractiveness to cybercriminals. The platform has become a fertile ground for malicious actors who exploit its features and users for various illegal activities. These cybercrimes range from phishing attacks and account hijackings to identity theft, scams, harassment, and data breaches. Criminals target both individuals and organizations, driven by motives that include financial gain, political agendas, personal vendettas, or mere disruption.

This paper seeks to explore the breadth and depth of cybercrime on Instagram. It investigates the types of crimes committed, the techniques employed by attackers, and the impact on victims and society. Additionally, it examines Instagram's existing security infrastructure, the legal frameworks in place to combat cybercrime, and the emerging trends that could shape the future of this digital battleground.

Given the rapidly evolving nature of cyber threats and the increasing integration of social media into daily life, understanding cybercrime on Instagram is not just important—it is essential. This research aims to equip readers with a thorough understanding of the challenges and provide informed insights and recommendations to enhance digital safety on the platform.

Overview of Instagram:

Instagram, launched in October 2010 by Kevin Systrom and Mike Krieger, has rapidly evolved from a simple photo-sharing app into one of the world's leading social media platforms. Acquired by Facebook (now Meta Platforms) in 2012, Instagram has continually expanded its features and user base, reaching over two billion active monthly users as of 2025.

At its core, Instagram is a visually focused platform where users can upload photos and videos, apply filters, and share their content with followers or the public. Beyond personal sharing, Instagram has grown into a powerful marketing and communication tool for businesses, influencers, and creators. Features like Stories, Reels, IGTV, and Shopping have transformed the platform into a dynamic ecosystem for engagement and e-commerce.

Instagram's design encourages interaction through likes, comments, direct messaging, and

sharing, fostering community building across diverse demographics worldwide. It supports a global audience with content spanning cultures, interests, and industries, making it a unique hub for connection and influence.

However, Instagram's vast popularity and diverse functionalities have also made it an attractive target for cybercriminals. The platform's rich user data, integration with business tools, and real-time communication features present both opportunities and vulnerabilities. Cybercriminals exploit these to conduct various malicious activities, ranging from identity theft and fraud to harassment and misinformation.

Understanding Instagram's structure, user behavior, and technological features is essential to grasp the nature and scope of cybercrime targeting the platform. This overview sets the stage for deeper exploration of how Instagram operates and why it is a focal point for digital threats.

Need for the Study:

The growing reliance on social media platforms, especially Instagram, has transformed the way individuals communicate, conduct business, and share personal information. However, this increased usage has also made users vulnerable to various forms of cybercrime such as hacking, phishing, impersonation, and financial fraud. Despite Instagram's efforts to strengthen its security infrastructure, the number of cybercrime incidents continues to rise, often going unreported or unresolved. Many users, particularly young people and small businesses, lack awareness of potential threats and the tools available to protect themselves. This study is necessary to understand the scope and nature of cybercrime on Instagram, evaluate the awareness levels of users, and identify gaps in existing safety measures. By exploring real-world user experiences through empirical data collection, this research aims to contribute to the growing discourse on digital safety and provide insights that can support preventive strategies, policy formulation, and user education.

Scope of the Study:

The scope of this study encompasses the analysis of cybercrime specifically targeting Instagram, including its users, infrastructure, and content. The study seeks to explore both the technical and social dimensions of cybercrime in the context of this platform. It aims to highlight the threats, consequences, and countermeasures related to malicious activities on Instagram.

Significance of the Study:

This study is significant because it helps to understand the growing threat of cybercrime on Instagram and how it affects everyday users. With the rise in online scams, account hacking, and impersonation, many users—especially youth, influencers, and small business owner face serious risks to their privacy, identity, and finances. By collecting data directly from Instagram users, this research highlights real-life experiences and reveals the level of awareness among users about online threats. The findings of this study can help social media platforms, cybersecurity agencies, educators, and policymakers design better safety features, awareness programs, and preventive measures. It also contributes valuable information to the field of cyber law and digital safety, making it useful for future researchers and legal practitioners.

Objectives of the Study:

The primary aim of this study is to analyse and understand the various dimensions of cybercrime as it relates to Instagram. The specific objectives are:

1. To identify and classify the major types of cybercrimes occurring on Instagram, such as phishing, impersonation, scams, and account takeovers.
2. To examine the key factors that make Instagram users vulnerable to cyber-attacks, including user behaviour, lack of awareness, and platform-specific weaknesses.
3. To assess the psychological, financial, and reputational impact of cybercrime on victims, including individuals, influencers, and businesses.
4. To evaluate the effectiveness of Instagram's current security features and policies in preventing and responding to cybercrime.
5. To explore the role of legal frameworks and enforcement agencies in combating cybercrime on social media platforms.
6. To provide recommendations for improving user safety, including awareness strategies, digital literacy, and policy reforms.
7. To suggest ways Instagram can strengthen its cybercrime prevention systems, including technological upgrades and better user support mechanisms.

Understanding Cybercrime:

Cybercrime, broadly defined, encompasses any illegal activity conducted through or facilitated by computers and the internet. As technology has become deeply integrated into daily life, cybercrime has evolved into a multifaceted threat that targets individuals, organizations, and governments alike. Unlike traditional crimes, cybercrime exploits the virtual realm, often

transcending geographic boundaries and complicating enforcement and prevention efforts.

At its core, cybercrime includes a wide array of offenses such as hacking, identity theft, online fraud, cyberstalking, ransomware attacks, and the distribution of malicious software. The motivation behind these crimes varies—some are financially driven, others politically motivated, while some aim to cause disruption or spread misinformation.

In the context of social media platforms like Instagram, cybercrime takes on unique characteristics. The platform's open and interactive nature creates an environment where attackers can exploit trust, access personal data, and manipulate user behavior. Cybercriminals leverage social engineering techniques, such as phishing and impersonation, to deceive users into revealing sensitive information or performing actions that compromise their security.

Furthermore, the vast amounts of data shared on Instagram—ranging from personal photos and locations to contact information and behavioral patterns—make it a rich target for data mining and privacy breaches. The ability to create anonymous or fake profiles enables malicious actors to harass, defraud, or impersonate others with relative ease.

Understanding cybercrime requires not only recognizing these diverse tactics and threats but also appreciating the complexities of the digital landscape where such crimes occur. [1]This section lays the foundation for comprehending how cybercrime manifests on Instagram and why it poses significant challenges to users, platform operators, and law enforcement agencies.

Cybercrime in the Context of Social Media:

Social media platforms like Instagram have revolutionized how people connect, communicate, and consume information. However, their global reach, real-time interaction, and vast data repositories also make them prime targets for cybercriminals. The very features that foster social engagement—such as instant messaging, public posting, and sharing personal details—can be manipulated to facilitate criminal activities.

Cybercrime on social media often exploits human psychology, using trust, curiosity, and social influence as vectors for attacks. For example, phishing scams might impersonate trusted contacts or well-known brands, tricking users into revealing credentials or clicking malicious links. The interconnected nature of social networks allows threats to propagate rapidly, amplifying their impact.

Additionally, social media platforms face unique challenges in moderating content and

[1] Boyd, D., & Ellison, N. B. (2007). Social Network Sites: Definition, History, and Scholarship. Journal of Computer-Mediated Communication, 13(1), 210–230. https://doi.org/10.1111/j.1083-6101.2007.00393.x

behaviour due to their scale and diversity. Automated bots can generate fake engagement or spread misinformation, while anonymous or fake profiles enable harassment and deception with little accountability.

The economic dimension is also significant: social media is a vital channel for marketing and commerce, attracting cybercriminals who exploit these ecosystems for financial gain. Scams involving fake promotions, fraudulent transactions, or counterfeit goods have become increasingly prevalent.

Understanding cybercrime within the social media context is essential to developing effective strategies for prevention, detection, and response. Instagram's role as a visually-oriented, widely used platform places it at the forefront of these challenges, where safeguarding users requires balancing openness with security**.**

What is Instagram and History:

Instagram is an American photo and short-form video sharing social networking service owned by Meta Platforms. It allows users to upload media that can be edited with filters, be organized by hashtags, and be associated with a location via geographical tagging. Posts can [2]be shared publicly or with preapproved followers. Users can browse other users' content by tags and locations, view trending content, like photos, and follow other users to add their content to a personal feed. A Meta-operated image-centric social media platform, it is available on iOS, Android, Windows 10, and the web. Users can take photos and edit them using built-in filters and other tools, then share them on other social media platforms like Facebook. It supports 32 languages including English, Hindi, Spanish, French, Korean, and Japanese.

Instagram was originally distinguished by allowing content to be framed only in a square (1:1) aspect ratio of 640 pixels to match the display width of the iPhone at the time. In 2015, this restriction was eased with an increase to 1080 pixels. It also added messaging features, the ability to include multiple images or videos in a single post, and a Stories feature—similar to its main competitor, Snapchat, which allowed users to post their content to a sequential feed, with each post accessible to others for 24 hours. As of January 2019, Stories was used by 500 million people daily.

Instagram was launched for iOS in October 2010 by Kevin Systrom and Mike Krieger. It rapidly gained popularity, reaching 1 million registered users in two months, 10 million in a year, and

[2] https://en.m.wikipedia.org/wiki/Instagram
Boyd, D., & Ellison, N. B. (2007). Social Network Sites: Definition, History, and Scholarship. Journal of Computer-Mediated Communication, 13(1), 210–230. https://doi.org/10.1111/j.1083-6101.2007.00393.x

1 billion in June 2018. In April 2012, Facebook acquired the service for approximately US$1 billion in cash and stock. The Android version of Instagram was released in April 2012, followed by a feature-limited desktop interface in November 2012, a Fire OS app in June 2014, and an app for Windows 10 in October 2016. Although often admired for its success and influence, Instagram has also been criticized for negatively affecting teens' mental health, its policy and interface changes, its alleged censorship, and illegal and inappropriate content uploaded by users.

Instagram began development in San Francisco as Burbn, a mobile check-in app created by Kevin Systrom and Mike Krieger. On March 5, 2010, Systrom closed a $500,000 (equivalent to $682,200 in 2023) seed funding round with Baseline Ventures and Andreessen Horowitz while working on Burbn. Realizing that it was too similar to Foursquare, they [3]refocused their app on photo-sharing, which had become a popular feature among its users. They renamed it Instagram, a portmanteau of instant camera and telegram.

2010–2011: Beginnings and major funding Josh Riedel joined the company in October as Community Manager, Shayne Sweeney joined in November as an engineer,and Jessica Zollman joined as a Community Evangelist in August [4]2011.

The first Instagram post was a photo of South Beach Harbor at Pier 38, posted by Mike Krieger at 5:26 p.m. on July 16, 2010. On October 6, 2010, the Instagram iOS app was officially released through the App Store. In February 2011, it was reported that Instagram had raised $7 million (equivalent to $9,357,057 in 2023) in Series A funding from a variety of investors, including Benchmark Capital, Jack Dorsey, Chris Sacca (through Capital fund), and Adam D'Angelo. The deal valued Instagram at around $20 million. In April 2012, Instagram raised $50 million (equivalent to $65,610,000 in 2023) from venture capitalists with a valuation of $500 million (equivalent to $656,100,000 in 2023). Joshua Kushner was the second largest investor in Instagram's Series B fundraising round, leading his investment firm, Thrive Capital, to double its money after the sale to Facebook.

2012–2014: Additional platforms and acquisition by Facebook

On April 3, 2012, Instagram released a version of its app for Android phones, and it was

[3] Boyd, D., & Ellison, N. B. (2007). Social Network Sites: Definition, History, and Scholarship. Journal of Computer-Mediated Communication, 13(1), 210–230. https://doi.org/10.1111/j.1083-6101.2007.00393.x

[4] https://en.m.wikipedia.org/wiki/Instagram

Boyd, D., & Ellison, N. B. (2007). Social Network Sites: Definition, History, and Scholarship. Journal of Computer-Mediated Communication, 13(1), 210–230. https://doi.org/10.1111/j.1083-6101.2007.00393.x

downloaded more than one million times in less than one day. The Android app has since received two significant updates: first, in March 2014, which cut the file size of the app by half and added performance improvements; then in April 2017, to add an offline mode that allows users to view and interact with content without an Internet connection. At the time of the announcement, it was reported that 80% of Instagram's 600 million users were located outside the U.S., and while the aforementioned functionality was live at its announcement, Instagram also announced its intention to make more features available offline, and that they were "exploring an iOS version". On April 9, 2012, Facebook, Inc. (now Meta Platforms) bought Instagram for $1 billion (equivalent to $1,312,000,000 in 2023) in cash and stock, with a plan to keep the company independently managed. Britain's Office of Fair Trading approved the deal on August 14, 2012, and on August 22, 2012, the Federal Trade Commission in the U.S. closed its investigation, allowing the deal to proceed. On September 6, 2012, the deal between Instagram and Facebook officially closed with a purchase price of $300 million in cash and 23 million shares of stock.

The deal closed just before Facebook's scheduled initial public offering according to CNN. The deal price was compared to the $35 million Yahoo! paid for Flickr in 2005. Mark Zuckerberg said Facebook was "committed to building and growing Instagram independently". [5]According to Wired, the deal netted Systrom $400 million.

In November 2012, Instagram launched website profiles, allowing anyone to see user feeds from a web browser with limited functionality, as well as a selection of badges, and web widget buttons to link to profiles. Since the app's launch it had used the Foursquare API technology to provide named location tagging. In March 2014, Instagram started to test and switch the technology to use Facebook Places.

mid-2022, Instagram introduced Notes in December 2022. This feature allows users to share updates as short text posts of up to 60 characters with certain people, who can then reply to them using messaging on Instagram.

Why Instagram is a Target:

Instagram’s immense popularity and broad user base make it an attractive target for cybercriminals. With over two billion active users globally, the platform hosts a diverse range of individuals—from casual users and influencers to major brands and businesses—each presenting unique opportunities for exploitation.

[5] https://en.m.wikipedia.org/wiki/Instagram

One key reason Instagram is targeted is the richness of user data. Profiles often contain personal information such as names, locations, birthdays, contact details, and social connections. This data can be harvested for identity theft, targeted phishing campaigns, or sold on illicit markets. The visual nature of Instagram also means users often share lifestyle details that can be exploited for social engineering attacks.

Moreover, Instagram's integration with e-commerce and advertising tools creates avenues for financial crimes. Businesses use the platform to reach customers, making fraudulent activities such as fake promotions, counterfeit sales, and payment scams lucrative for criminals. Influencers and celebrities are frequent targets for account takeovers, which can be monetized by spreading scams or selling access to followers.

The platform's interactive features—direct messaging, Stories, comments, and live broadcasts—facilitate rapid communication, but also allow cybercriminals to spread malware, [6]phishing links, and misinformation quickly. Additionally, the relative anonymity provided by the internet enables the creation of fake profiles and bots, which can impersonate others, spread disinformation, or manipulate engagement metrics.

[7]Finally, Instagram's status as a cultural and social hub means cybercrime on the platform can have a significant psychological and reputational impact on victims, encouraging more malicious actors to exploit these vulnerabilities.

In summary, Instagram's combination of vast user engagement, valuable data, financial tools, and interactive capabilities makes it a prime target for a wide spectrum of cybercriminal activities.

Phishing Attacks on Instagram

Phishing is one of the most pervasive and effective cybercrime tactics used against Instagram users. It involves deceiving victims into providing sensitive information, such as login credentials, personal data, or financial details, by masquerading as a trustworthy entity.

On Instagram, phishing attacks often take several forms:

- Fake Login Pages: Attackers create websites or pop-ups that look identical to Instagram's official login page. Unsuspecting users are tricked into entering their username and password, which the attacker then captures and uses to compromise the

[6] https://en.m.wikipedia.org/wiki/Instagram
Boyd, D., & Ellison, N. B. (2007). Social Network Sites: Definition, History, and Scholarship. Journal of Computer-Mediated Communication, 13(1), 210–230. https://doi.org/10.1111/j.1083-6101.2007.00393.x

account.

- Direct Message Scams: Cybercriminals send fraudulent direct messages (DMs) pretending to be Instagram support, popular influencers, or friends. These messages may contain links that lead to phishing sites or urge the user to share private information.
- Email Phishing: Although Instagram primarily uses in-app notifications, users may receive emails that appear to come from Instagram, warning them of suspicious activity or offering urgent account recovery. These emails often contain malicious links.
- Third-Party Apps and Services: Some phishing scams encourage users to log in through unauthorized apps promising free followers, likes, or other perks. These apps harvest login data and compromise user accounts.

The consequences of phishing attacks are severe. Victims often lose access to their accounts, suffer identity theft, and experience privacy violations. Compromised accounts can be used to perpetrate further scams, spreading phishing attempts to the victim's followers.

Combatting phishing requires a combination of user awareness, technological safeguards like two-factor authentication (2FA), and Instagram's efforts to detect and block fraudulent content. Educating users about common phishing tactics and encouraging skepticism toward unsolicited messages are critical components of defense.

Hypothesis:

"Despite the availability of security features on Instagram, users continue to face significant cyber threats due to inadequate platform response, lack of user awareness, and insufficient trust in Instagram's privacy measures."

Does the fear of embarrassment or social stigma prevent Instagram users from reporting cybercrime incidents, such as account hacking or impersonation, to authorities or the platform?

Answer (Hypothesis): Yes, many Instagram users avoid reporting cybercrime incidents due to feelings of shame, fear of reputational damage, or the belief that reporting will not lead to effective resolution.

Review of literature:

Research on cybercrime against social media users has consistently revealed an alarming rise in security breaches, fraud, and user exploitation. According to NCRB (2022), cybercrime complaints related to social media have steadily increased, with Instagram among the most

reported platforms due to its high engagement levels. Sharma (2021) observed that Instagram users—especially influencers and small business owners—are frequent targets of phishing attacks and impersonation scams. Kumar & Rathi (2020) studied the exploitation of Instagram's direct messaging and story features for spreading malicious links, which often lead to data theft and account hacking.

CERT-In (2021) issued multiple advisories about rising threats on social media, identifying fake pages, fraudulent promotions, and malware-spreading links as primary methods used by cybercriminals. Meena (2019) emphasized the vulnerabilities associated with third-party applications linked to Instagram, pointing out that many users unknowingly grant access to personal data. Singh & Dey (2022) highlighted that cybercrime affects not only individual users but also impacts digital marketing agencies and brand collaborations due to loss of credibility and account control.

Chakraborty (2023) emphasized the need for digital literacy among teenagers, who are particularly susceptible to scams through fake giveaways and influencer impersonation. Across these studies, a common recommendation is the integration of user education, platform-level security updates, and government-led awareness campaigns to curb the impact of such crimes.

Research Gap:

While prior studies on social media cybercrime have largely focused on general user behaviour or technical vulnerabilities, there is a lack of real-time user-generated data assessing how Instagram users personally experience and respond to cyber threats. This survey fills that gap by providing direct insights from users about their trust in Instagram's privacy settings, their encounters with fake profiles, scams, and cyberbullying, and the preventive actions they take. Moreover, there is limited research exploring the emotional and psychological impact of these threats in combination with perceptions of Instagram's security efforts—something your data begins to uncover.

Research Problem:

This research investigates the growing concern of cybercrime on Instagram, focusing on users' experiences with privacy threats, hacking, phishing, cyberbullying, and impersonation. Despite Instagram being one of the most widely used social media platforms, user responses indicate a serious gap between the platform's perceived security features and actual user trust. The study aims to identify the level of cybersecurity awareness among users and evaluate the effectiveness of Instagram's safety measures from the user perspective.

Research Methedology:

This study is based on non-doctrinal(empirical) research methodology, which involves the collection and analysis of primary data to understand the real-world impact of cybercrime on Instagram users. The research was conducted using a structured questionnaire distributed via Google Forms to a diverse group of Instagram users. The objective of the survey was to gather firsthand information about users' experiences with cyber threats such as phishing, account hacking, scams, and impersonation. The questionnaire included both closed-ended and open-ended questions, allowing for both quantitative data and qualitative insights. Respondents were selected using purposive sampling, focusing on individuals who actively use Instagram. The data collected from the responses were analysed to identify patterns in user awareness, frequency of cyber incidents, types of threats encountered, and the effectiveness of Instagram's security features. The findings aim to reflect the real-time challenges faced by users and to assess whether current preventive measures are sufficient. This empirical approach enables the study to present a grounded understanding of cybercrime on Instagram, supported by data derived directly from user experiences.

Research Questions:

1. What are the most common types of cybercrime committed on Instagram?
2. Who are the primary targets of Instagram-related cybercrimes, and why?
3. What are the psychological, financial, and reputational impacts of these crimes on victims?
4. How effective are Instagram's current security measures in preventing or mitigating cybercrime?
5. To what extent are Instagram users aware of potential cyber threats and security best practices?
6. What improvements can be made to user education, policy enforcement, and platform design to reduce cybercrime?

CHAPTERISATION

Chapter 1

The most common types of cybercrime committed on Instagram

Instagram, being one of the most popular social media platforms globally, has also become a hotspot for various types of cybercrimes. These crimes exploit both technical vulnerabilities and human behaviour, often resulting in significant emotional, financial, or reputational damage for the users. The most common forms include:

Types of Cybercrime Against Instagram:

1. **Phishing Attacks**

   Phishing is a common tactic where attackers deceive users into revealing sensitive information like passwords or financial details. On Instagram, phishing often occurs through direct messages, fake emails, or counterfeit login pages that mimic Instagram's official interface.

2. **Account Takeovers and Credential Theft**

   Cybercriminals use stolen credentials obtained via phishing, data breaches, or malware to hijack Instagram accounts. Once in control, they can lock out the legitimate owner, impersonate them, spread scams, or sell access to followers and personal data.

3. **Fake Profiles and Impersonation**

   Creating fraudulent accounts that impersonate real users, celebrities, or brands is widespread. [7]These fake profiles can be used to scam followers, spread misinformation, or engage in harassment and defamation.

4. **Instagram Scams and Fraudulent Schemes**

   Scammers exploit the trust users place in the platform through fake giveaways, investment opportunities, or requests for donations. These schemes often trick users into sending money or divulging confidential information.

5. **Cyberbullying and Harassment**

   Instagram users,especially younger demographics, face harassment through threatening messages, hate speech, and public shaming. Cyberbullying can have severe emotional and psychological consequences for victims.

6. **Content Piracy and Copyright Violations**

   Unauthorized reposting or use of copyrighted content without permission undermines

[7] Instagram Help Center. (n.d.). Privacy and Security Help. Retrieved from https://help.instagram.com/

creators' rights and income. This form of cybercrime is difficult to police given the volume of content shared daily.

7. **Data Mining and Privacy Breaches**

   Attackers gather personal and behavioral data from public and private posts to build profiles for identity theft or targeted attacks. Privacy breaches often occur through unauthorized access or exploitation of platform vulnerabilities.

8. **Bot Activity and Fake Engagement**

   Automated bots are used to generate fake likes, comments, and followers, misleading users and brands about popularity and influence. Bots also facilitate the spread of spam and malicious [9]links.

   Each of these cybercrimes poses unique challenges for Instagram's security teams and users alike. The complexity and sophistication of attacks continue to evolve, necessitating robust defenses and ongoing vigilance.

Chapter 2

Who are the primary targets of Instagram-related cybercrimes, and why?

Cybercriminals on Instagram often target users who are more vulnerable due to their online behavior, visibility, or lack of awareness about digital security. The primary targets include:

1. **Influencers and Public Figures**

   Influencers, celebrities, and public figures are prime targets because of their large following and the potential impact of misusing their accounts. Hackers often hijack influencer accounts to promote scams, send phishing messages, or demand ransom in exchange for account recovery. Since these accounts generate income and influence public opinion, they become attractive assets for cybercriminals.

2. **Small Business Owners and Entrepreneurs**

   Many small businesses use Instagram as a primary platform for marketing, customer engagement, and direct sales. Cybercriminals exploit this by impersonating business pages, hijacking accounts, or sending fraudulent order requests. Loss of access to their business account can severely affect their operations and credibility, making them vulnerable to extortion.

3. **Teenagers and Young Adults**

   Young users are often less aware of cyber threats and more likely to fall for scams like fake giveaways, love scams, or follower-boosting services. Their tendency to share

personal information online, use weak passwords, or trust unknown users makes them easy targets for phishing, harassment, or identity theft.

4. **New or Inexperienced Users**

   People who are new to Instagram may not fully understand how to spot fake messages [8]or configure their privacy settings. These users may unknowingly click on harmful links, respond to scam messages, or grant access to suspicious third-party apps, exposing themselves to threats.

5. **Women and Minority Groups**

   Women, particularly those with public profiles, often face targeted harassment, stalking, or blackmail. In some cases, personal photos are misused or shared without consent. Minority groups may also be targeted through hate speech or identity-based attacks.

6. **High-Net-Worth or Verified Accounts**

   Accounts with verified status or visible signs of wealth (luxury lifestyles, expensive brands) attract cybercriminals who assume these users are more likely to pay ransoms or fall for investment scams. Their credibility is also misused to deceive their followers.

Why These Groups Are Targeted:

Visibility: The more visible a user is, the more value their account holds for scammers.

Trust Factor: Followers are more likely to trust messages from known or verified accounts.

Lack of Awareness: Younger or inexperienced users may not recognize scam signs.

Financial Motive: Business accounts and influencers are often linked to earnings, increasing their vulnerability to extortion.

Ease of Manipulation: Emotional manipulation, urgency tactics, or technical tricks are often successful with unaware or trusting users.

Chapter 3

What are the impacts of Instagram-related cybercrime on victims, both psychologically and financially?

Instagram-related cybercrimes have a wide range of consequences for victims, affecting them not only financially but also emotionally and psychologically. These impacts can be immediate or long-term, depending on the severity of the attack and the victim's personal or professional connection to their Instagram account.

[8] Instagram Help Center. (n.d.). Privacy and Security Help. Retrieved from https://help.instagram.com/

A. Psychological Impacts

1. Stress and Anxiety

Victims often experience high levels of stress and anxiety after falling prey to cybercrime. This is especially true in cases of account hacking, impersonation, or online harassment. The fear of losing control over personal data, photos, or private messages can be deeply unsettling. Many users feel violated, unsafe, and paranoid about further attacks.

2. Loss of Trust and Confidence

When users become victims of scams, phishing, or identity theft, they often lose trust not only in Instagram but in digital platforms in general. They may become hesitant to use social media, share personal updates, or interact with strangers. This lack of confidence can reduce their social engagement and online activity, especially if their online identity was central to their personal or professional life.

3. Embarrassment and Social Shame

Victims of certain types of cybercrime—such as fake posts made from their hacked accounts, misuse of personal photos, or falling for fake giveaways—may feel embarrassed or ashamed. This emotional burden can discourage them from reporting the incident or seeking [9]help, especially if they believe they'll be judged for being "careless."

4. Mental Health Decline

In severe cases, cyberbullying or harassment on Instagram can lead to depression, isolation, or suicidal thoughts—especially among teenagers. Continuous exposure to abusive messages, threats, or blackmail can have a serious and lasting effect on mental health.

B. Financial Impacts

1. Loss of Money Due to Scams

Victims of Instagram-based scams often lose money through fake investment schemes, counterfeit online sales, or fraudulent job offers. These scams usually appear convincing and are promoted through hijacked or fake accounts that mimic real users or brands. Once users send payments or share sensitive financial information, the scammers disappear, leaving no chance of recovery.

[9] https//:www.researchgate.net

2. **Business Disruption**

   For entrepreneurs, influencers, or small business owners, a hacked or disabled account can halt business operations. Orders may be missed, client communications lost, and trust damaged. Recovering a business account takes time, and in many cases, the account may not be recovered at all, resulting in a direct loss of income and professional reputation.

3. **Expenses in Recovery**

   Victims may have to spend money on professional help, such as hiring cybersecurity experts, legal advisors, or social media consultants, to recover their accounts or manage the damage. In cases of severe identity theft or impersonation, legal proceedings can also involve court or lawyer fees.

4. **Loss of Opportunities**

   When an Instagram account is compromised, users may miss out on promotional deals, brand collaborations, or job offers. Influencers, in particular, depend on their Instagram [10]presence for visibility and income, and any disruption can affect their growth and earnings.

C. Social and Reputational Impact

1. **Damage to Personal Reputation**

   If a hacker uses a victim's account to post offensive content, scam others, or spread misinformation, the victim's reputation can be seriously damaged. Friends, followers, or business partners might assume the victim is responsible for the inappropriate content.

2. **Strained Relationships**

   Being a victim of cybercrime can affect one's personal relationships, especially if private information is leaked or if others were scammed through the victim's account. It can create tension, blame, or mistrust among close contacts.

Conclusion

The impacts of Instagram-related cybercrime go beyond just technical inconvenience—they often leave victims feeling emotionally drained, socially isolated, and financially insecure. While Instagram offers some tools for reporting and recovery, these are not always fast or

[10] https//: www.researchgate.net

effective. This underlines the need for better support systems, user education, and legal mechanisms to help victims recover and regain confidence in using the platform safely.

Chapter 4

How effective are Instagram's current security features and user support systems in preventing or addressing cybercrime?

Instagram has developed a range of security features and support systems aimed at protecting users from cybercrime. While these tools offer basic protections and help in many cases, their effectiveness is still limited by technical gaps, user awareness, and the evolving nature of cyber threats. The platform continues to improve its safety protocols, but challenges remain, especially when it comes to swift response and accessibility.

A. Instagram's Current Security Features

1. **Two-Factor Authentication (2FA)**

   Instagram allows users to enable 2FA, which adds an extra layer of protection during login by requiring a code sent to the user's phone or authentication app. This helps prevent unauthorized access even if login credentials are stolen.

2. **Login Activity Monitoring**

   Users can view their login history and recognize suspicious logins. If an unfamiliar device is detected, users are advised to change their password immediately.

3. **Report and Block Features**

   Instagram allows users to block, restrict, or report abusive accounts, spam messages, phishing attempts, and impersonation. These reports are reviewed by the Instagram moderation team.

4. **Support for Hacked Accounts**

   Instagram provides a recovery process for hacked accounts, including identity verification through email, phone number, or even selfies. However, this process can be slow and frustrating, especially for users without access to linked recovery options.

5. **Privacy Settings**

   Instagram offers users options to make their accounts private, control who can comment or send messages, and filter offensive content. These tools help users limit exposure to strangers and reduce the risk of harassment.

6. **Educational Alerts and Warnings**

   Instagram has begun showing warnings when users interact with potentially harmful

content, such as phishing links or spammy DMs. Users are also shown prompts about strong password usage and safe practices.

B. Limitations of Instagram's Security Measures

1. **Slow Account Recovery Process**

   Many users report that the account recovery system is not efficient. Victims often struggle to regain access to hacked accounts, and in some cases, may never recover them. The process relies heavily on automated responses, which can delay support for urgent issues.

2. **Inadequate Human Support**

   Instagram lacks real-time customer support or direct contact with a help desk. Victims of cybercrime often face difficulties when trying to explain complex issues or when they are not tech-savvy.

3. **Over-Reliance on User Reports**

   Much of Instagram's response to cybercrime depends on users reporting inappropriate behavior or suspicious accounts. This reactive model allows many scams or fake accounts to stay active for extended periods before being addressed.

4. **Scalability of Threat Detection**

   With billions of users, it is challenging for Instagram to detect and prevent every cyber threat. Automated moderation can miss sophisticated phishing attempts or scams that appear genuine on the surface.

5. **Lack of Awareness Among Users**

   Even with security features available, many users are unaware of how to use them. Young or inexperienced users often fail to enable 2FA, ignore suspicious behaviour, or fall for scams because they don't recognize the warning signs.

C. Areas for Improvement Introducing Real-Time Support

Adding human support channels—such as chatbots with escalation options or live help for hacked accounts—would make recovery faster and more accessible.

Stronger AI for Scam Detection

Instagram could invest more in artificial intelligence to detect and shut down scam accounts before they can reach victims.

User Education Campaigns

Regular awareness campaigns, especially targeting youth and small business owners, [11]could help reduce victimization by promoting safer digital behaviour.

More Transparent Reporting Feedback

When users report issues, they rarely receive detailed updates about the status of their reports. Transparency could help build trust and encourage more users to report.

Conclusion

Instagram's current security and support systems offer important tools to prevent cybercrime, but they are not yet fully effective. Many users still fall victim due to slow support, lack of awareness, or technical weaknesses. To address this, Instagram needs to invest in faster recovery systems, better education, and more proactive monitoring tools to ensure users feel safe and supported.

Chapter 5

What legal measures and policies are in place to combat Instagram-related cybercrime in India, and how effective are they?

In India, the legal framework to combat cybercrime—including offenses committed on platforms like Instagram—is primarily governed by the Information Technology Act, 2000 (IT Act), along with relevant provisions of the Indian Penal Code (IPC). These laws provide the foundation for addressing various forms of cybercrime, including identity theft, hacking, online harassment, and financial fraud. However, enforcement and awareness remain key challenges in ensuring their effectiveness.

A. Legal Provisions Under Indian Law

1. Information Technology Act, 2000 (Amended in 2008)

The IT Act is the principal legislation for cyber offenses in India. Relevant sections include:

Section 66C:

Punishes identity theft and fraudulent use of electronic signatures or passwords (e.g.,

[11] Statista. (2023). Number of Instagram users worldwide from 2019 to 2023. Retrieved from https://www.statista.com/
Cybercrime.gov.in. (n.d.). Report and Track Cyber Crimes in India. Ministry of Home Affairs. https://www.cybercrime.gov.in/

impersonation on Instagram).

Section 66D:

Covers cheating by impersonation using computer resources—often applied in online job fraud and scam cases. Section 66E: Deals with violation of privacy, such as sharing private images or videos without consent.

Section 67:

Criminalizes the publishing or transmission of obscene material in electronic form, applicable to cases involving explicit content or online harassment.

Section 43 & 66:

Address unauthorized access to data (hacking) and damage to computer systems or networks.

2. Indian Penal Code (IPC) Provisions

The IPC is also used to prosecute Instagram-related offenses when applicable: Section 419 & 420: Pertaining to cheating, impersonation, and fraud.

Section 354D:

Stalking, including cyberstalking, which is often reported by women on Instagram.

Section 499 & 500:

Defamation, relevant to cases of false allegations or harmful content posted on Instagram.

Section 507:

Criminal intimidation by anonymous communication, used in cases of threats via messages or DMs.

3. IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

These rules make it mandatory for platforms like Instagram to: Appoint grievance officers for content-related complaints.

Take down unlawful or offensive content within a specific time.

Help law enforcement agencies by preserving data or identifying the origin of a message if required legally.

C. Effectiveness of Legal Measures

1. Strengths

The Indian legal system provides a broad legal basis to address various types of Instagram-related cybercrimes.

Victims have access to multiple reporting channels including cybercrime.gov.in, local police stations, and cyber cells.

Awareness about online fraud is growing, leading to increased reporting, especially in urban

areas.

2. Challenges

Lack of Awareness: Many victims, especially in rural or semi-urban areas, are unaware of their legal rights or how to report cybercrime.

Underreporting: Victims often do not report due to fear, embarrassment, or mistrust in the justice system.

Delayed Investigation: Law enforcement agencies are sometimes unequipped or understaffed to handle complex cyber cases swiftly.

Jurisdictional Issues: Cybercrimes can cross state and national boundaries, complicating investigations and prosecutions.

Platform Cooperation: Instagram, being a foreign platform, may delay or limit its cooperation with Indian authorities unless formal requests are made.

D. Recent Improvements and Initiatives Dedicated Cybercrime Portals and Helplines

The Government of India has launched cybercrime.gov.in for online complaint registration and a dedicated helpline (1930) for immediate financial fraud reporting.

Capacity Building

Several police forces are establishing cybercrime cells and offering training programs to build expertise in digital forensics and social media crime handling.

[12]Public Awareness Campaigns

Law enforcement agencies and non-profits have started conducting workshops and digital campaigns to educate citizens about common scams and how to stay safe online.

Conclusion

India has a well-defined legal structure to address Instagram-related cybercrimes, combining IT laws and criminal statutes. However, the effectiveness of these laws depends on public awareness, prompt action by authorities, and better cooperation with digital platforms.

[12] Statista. (2023). Number of Instagram users worldwide from 2019 to 2023. Retrieved from https://www.statista.com/
Cybercrime.gov.in. (n.d.). Report and Track Cyber Crimes in India. Ministry of Home Affairs. https://www.cybercrime.gov.in/

CASE LAWS:

1. Shreya Singhal v. Union of India (2015) 5 SCC 1 Facts:

The petitioner challenged the constitutional validity of Section 66A of the Information Technology Act, 2000, which allowed the arrest of individuals for posting "offensive" content online.

Relevance to Instagram Cybercrime:

This case is critical in protecting freedom of expression on social media, including Instagram. It also emphasized the importance of clear and non-arbitrary laws related to online communication. While the court struck down Section 66A, it reinforced that genuine cybercrimes like impersonation, threats, and stalking must be handled under other IT Act provisions.

2. Kalandi Charan Lenka v. State of Odisha (2017 SCC OnLine Ori 81) Facts:

A female student was subjected to cyberstalking, obscene messages, and threats through fake profiles on Facebook. The accused also shared morphed photos to harass the victim.

Relevance to Instagram:

This case reflects the growing issue of fake profiles and impersonation, a key concern found in your survey. It shows how courts treat the use of fake identities and harassment on social media seriously under Sections 66C, 66E, and 67 of the IT Act, along with IPC provisions.

3. Sabu Mathew George v. Union of India (2017) 2 SCC 514 Facts:

This case dealt with the misuse of online platforms to advertise illegal sex-determination tests, which were banned under Indian law.

Relevance:

Though not about Instagram directly, the Supreme Court emphasized the platforms' duty to monitor and remove illegal content, setting a precedent for accountability of social media platforms in preventing harmful or unlawful activities online.

4. State of Tamil Nadu v. Suhas Katti (2004) Facts:

This was one of the earliest cyberstalking cases in India. The accused posted obscene and defamatory messages about a woman on a Yahoo message board and created fake email accounts in her name.

Relevance to Instagram:

The case is foundational in dealing with cyber harassment, which parallels modern-day Instagram issues like cyberbullying, impersonation, and defamation through fake accounts and stories.

5. XYZ v. Instagram (Meta Platforms, Inc.) – (Hypothetical/Recent Petitions) Facts:

Although specific Indian Instagram cases are often underreported, there are increasing numbers of complaints filed through Cybercrime Portals about scams, identity theft, and image-based abuse on Instagram.

Relevance:

These cases emphasize the importance of user protection, the role of intermediaries, and the legal remedy available under IT Act Sections 66C, 66D, 67, and IPC Sections 354D (stalking), 509 (insulting modesty of a woman), etc.

Legal Framework Summary Relevant to Instagram Cases:

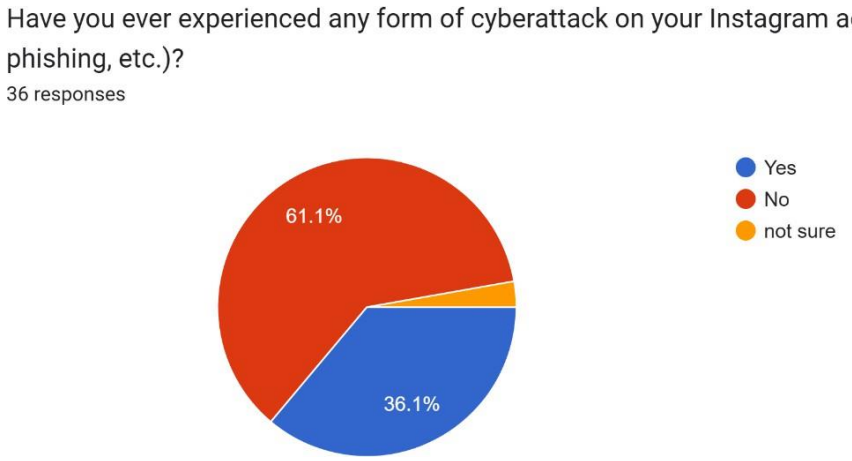
Section 66C – Identity theft

Section 66D – Cheating by personation via computer resources Section 67 – Publishing obscene content in electronic form Section 354D IPC – Cyberstalking

Section 509 IPC – Outraging the modesty of a woman

IT Intermediary Guidelines Rules (2021) – Duty of Instagram as a platform.

Manually evidence:



According to your survey, 36.1% of users have experienced some form of cyberattack on their

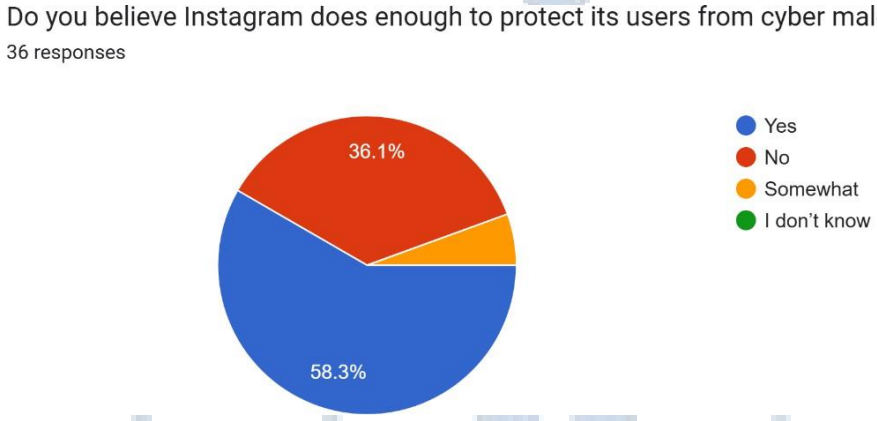
Instagram account, such as hacking or phishing. This shows that more than 1 in 3 users are affected, which is a serious issue.

To reduce this risk, it is suggested that:

Users should enable two-factor authentication to protect their accounts.

Instagram should improve its security features and warn users about phishing links.

Awareness programs should be conducted, especially for young users, to help them recognize suspicious messages or fake login pages.



This data highlights the need for better education and stronger security practices among Instagram users.

User Opinion on Instagram's Cybersecurity Measures

The chart shows the responses to the question:

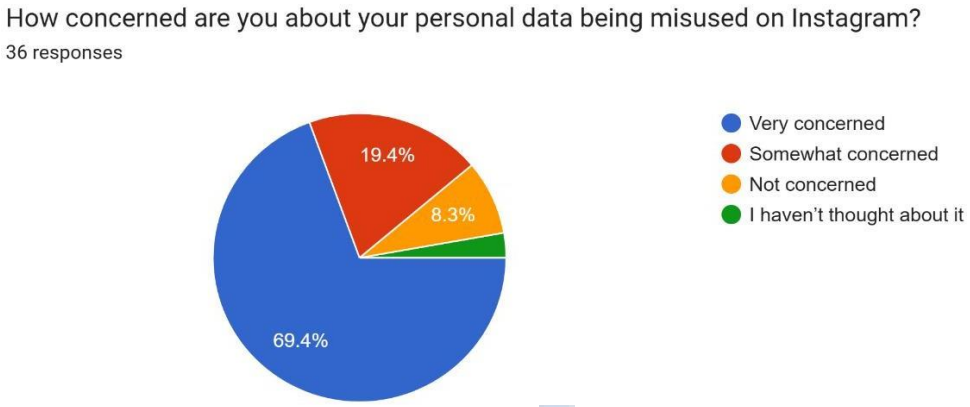
"Do you believe Instagram does enough to protect its users from cyber malefactions?" Key Findings from 36 Responses:

- 58.3% of participants said "Yes" – indicating that a majority of users believe Instagram provides enough protection against cyber threats.
- 36.1% said "No" – which shows that over one-third of users feel Instagram's efforts are not enough.
- 5.6% selected "Somewhat" – suggesting they think protection is only partially effective.
- 0% selected "I don't know" – meaning all participants had an opinion on this issue.

Interpretation:

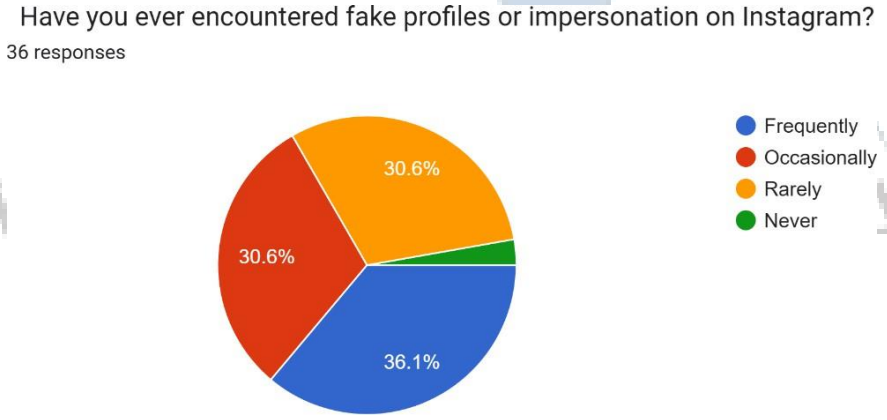
Although most users feel secure on Instagram, a significant 36.1% lack confidence in the

platform's ability to prevent cybercrimes like hacking, phishing, or data theft. This shows a need for improvement in security communication, user trust-building, and possibly adding more visible safety features.



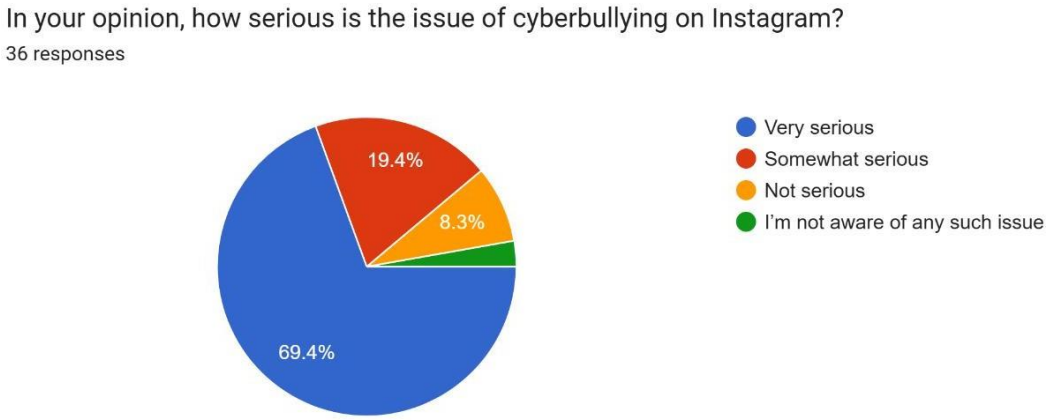
The chart shows that 69.4% of respondents are very concerned about their personal data being misused on Instagram. About 19.4% are moderately concerned, while 8.3% are slightly concerned.

A very small number showed little or no concern. This indicates that most users are highly worried about their data privacy on the platform.



Out of 36 responses, 36.1% of people said they frequently see fake profiles on Instagram. Another 30.6% encounter them occasionally, and 30.6% rarely.
Only a small number have never seen fake accounts.

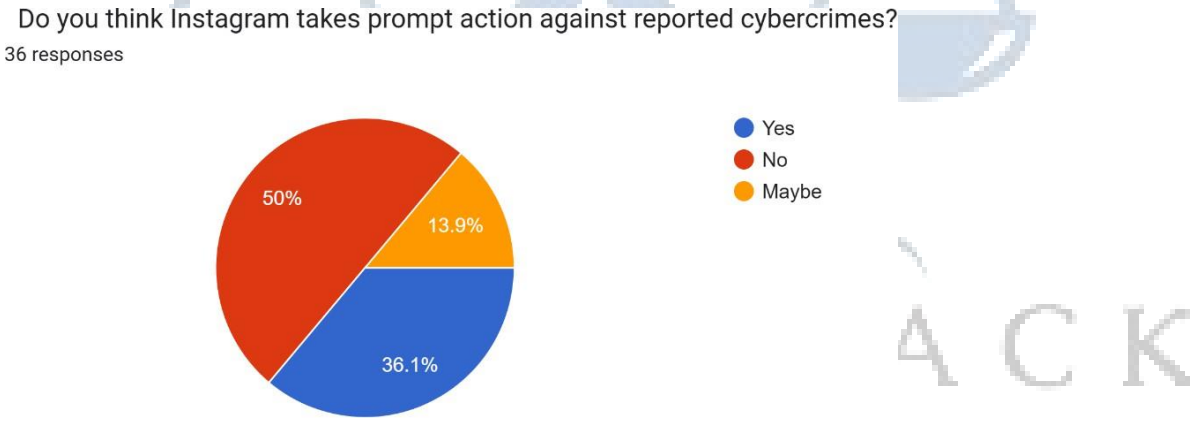
This indicates that impersonation is a common issue experienced by most users



According to the responses, 69.4% of users believe cyberbullying on Instagram is a very serious issue.

Around 19.4% consider it somewhat serious, while 8.3% think it's not serious. A small portion is unaware of such issues.

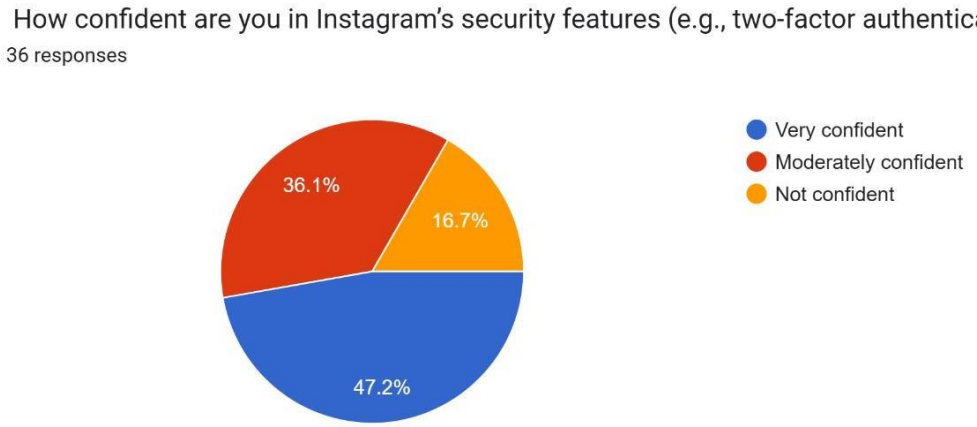
This suggests that most users recognize cyberbullying as a major concern on the platform.



The survey shows mixed opinions on Instagram's response to cybercrimes. Half of the respondents feel Instagram is not taking prompt action.

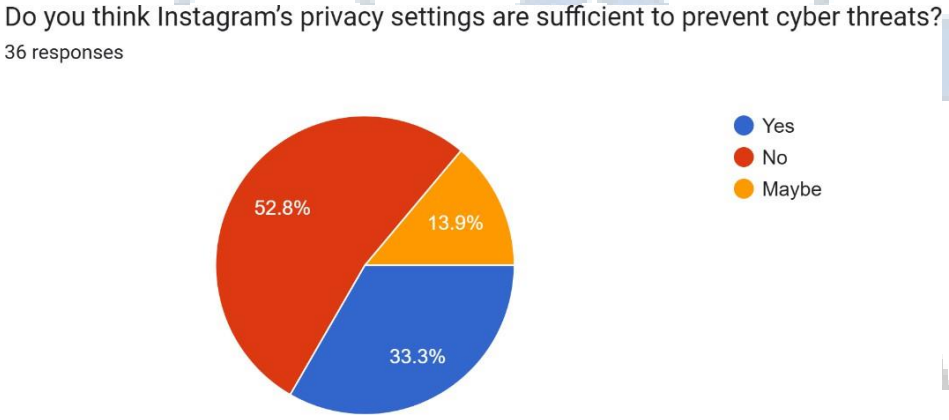
Only 36.1% believe the platform responds quickly to reports.

This indicates a need for Instagram to improve user trust and action efficiency.

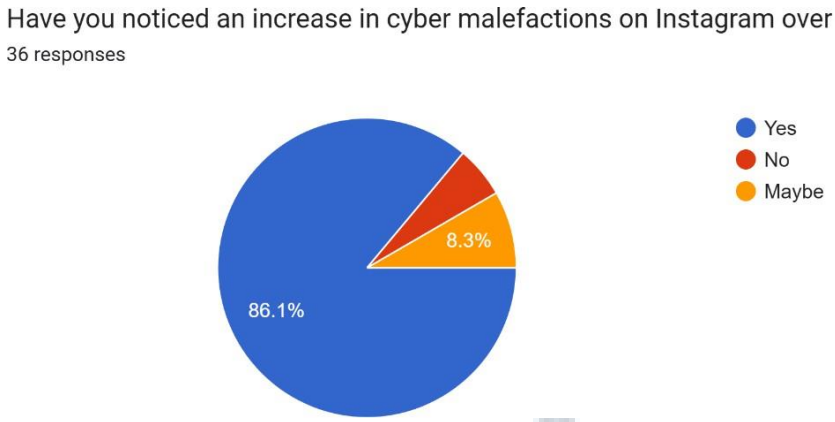


A significant 36.1% of users have faced scams or fraudulent links on Instagram. This suggests a notable level of risk for a large portion of users.

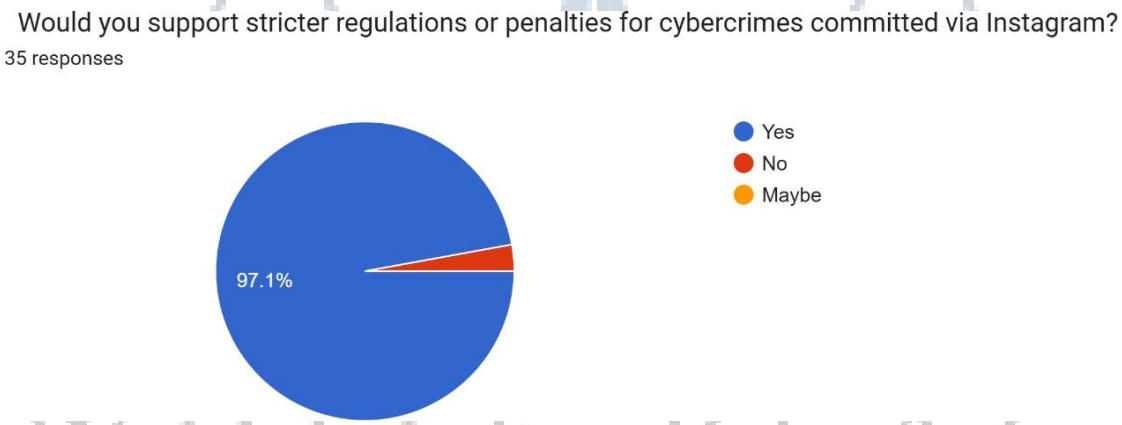
However, 63.9% have not encountered such threats, indicating mixed experiences. Stronger digital literacy and platform safeguards can reduce such incidents.



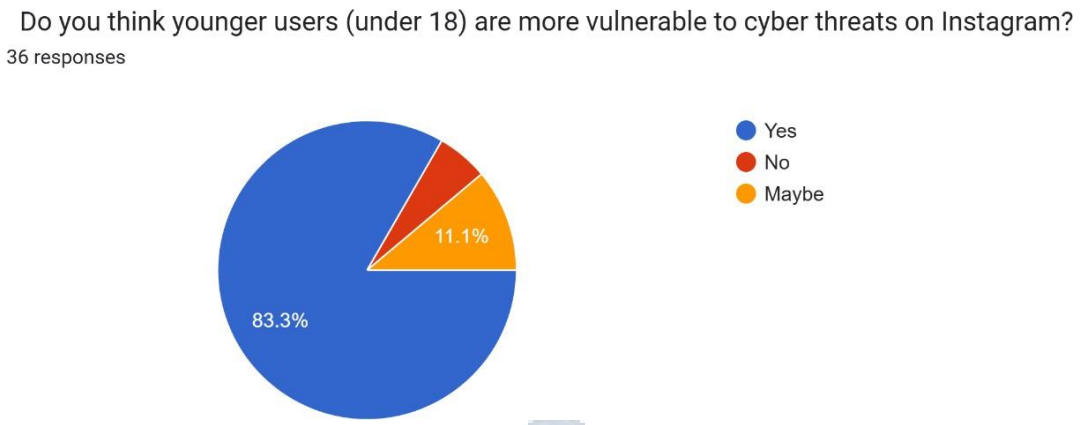
Instagram should enhance awareness about security tools like two-factor authentication. More user-friendly guidance can boost confidence in these safety features.



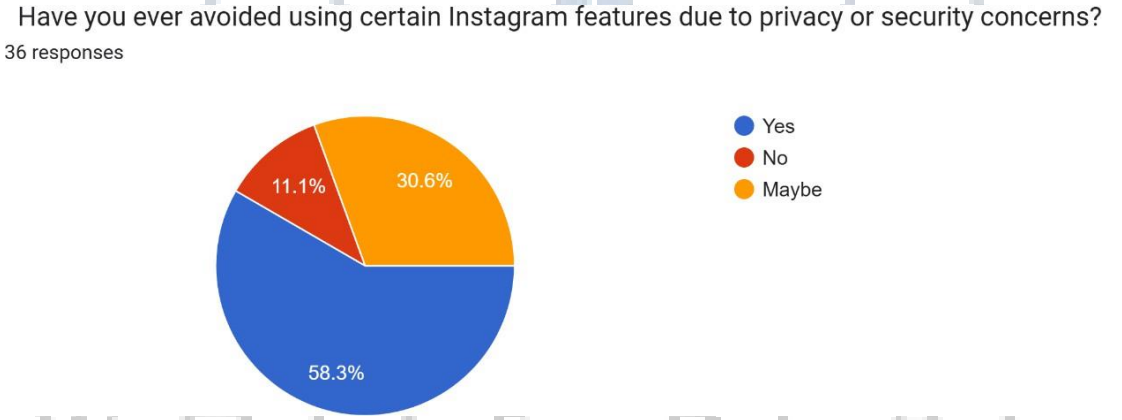
Out of 36 respondents, a significant majority—86.1%—answered Yes, indicating a clear perception of rising cyber threats on the platform. Only 5.6% said No, while 8.3% were uncertain. The data highlights growing public concern about Instagram's cyber safety.



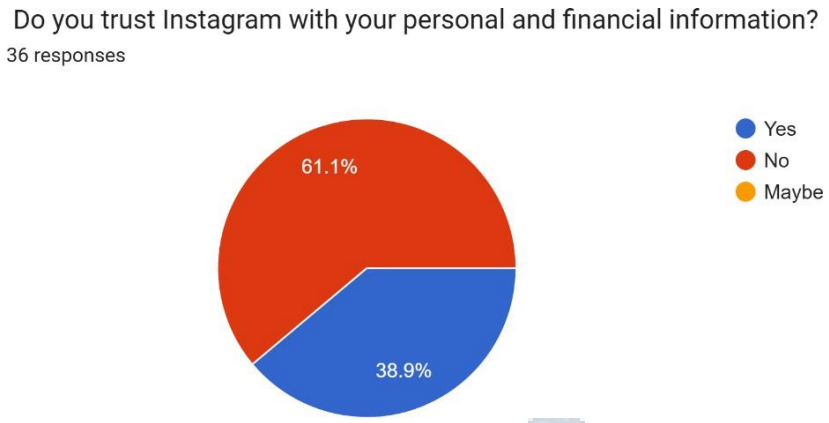
Out of 35 participants, an overwhelming 97.1% answered Yes, strongly favoring stricter measures. Only a small minority disagreed or were uncertain. This reflects a public demand for stronger legal action and accountability in handling Instagram-related cybercrimes.



Out of 36 respondents, 83.3% said Yes, suggesting that most people believe minors are at higher risk. Only 5.6% said No, and 11.1% were unsure. This highlights a strong concern for online safety among younger user.



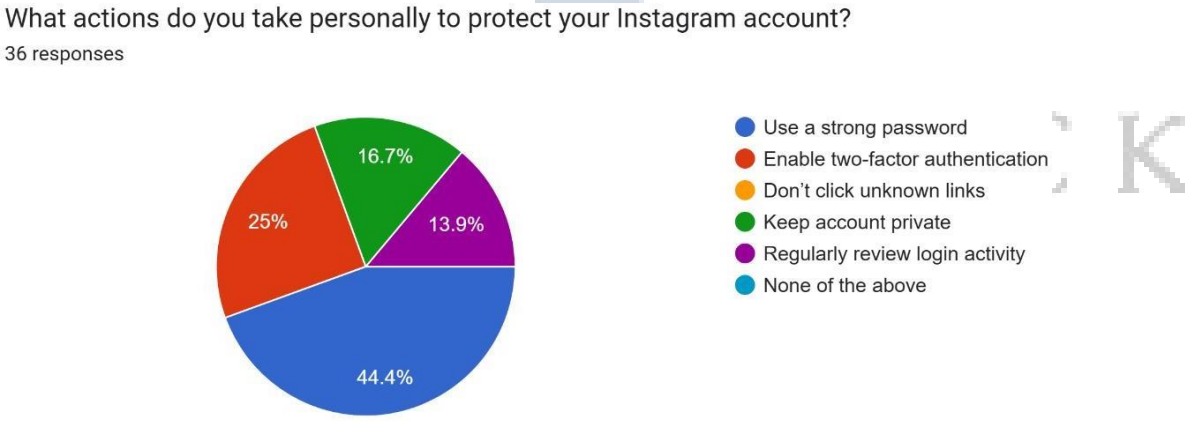
Out of 36 participants, 58.3% said Yes, showing a majority have privacy fears. 30.6% were unsure, and 11.1% said No, indicating that concerns over safety affect how many users engage with Instagram features.



From 36 respondents:

61.1% said No, showing most people do not trust Instagram with sensitive information. 38.9% said Yes, meaning a smaller portion does trust the platform.
There are no "Maybe" responses, indicating people have strong opinions on this matter.

Most users are concerned about Instagram's ability to keep their personal and financial data safe.



Out of 36 responses:

44.4% use a strong password (most common action). 25% enable two-factor authentication.
16.7% keep their account private. 13.9% regularly review login activity.
A small portion avoids clicking on unknown links, but exact percentage not shown here.

Very few or no one selected "None of the above," meaning most users take at least one security measure.

Conclusion: Most people actively take steps to protect their Instagram accounts, especially by using strong passwords and enabling two-factor authentication.

Survey Analysis

This non-doctrinal study is based on responses from 36 participants who shared their experiences and opinions related to cyber malefactions on Instagram. The survey aimed to identify users' exposure to cyber threats, their trust in Instagram's security, and their personal efforts to safeguard their accounts.

To begin with, 36.1% of respondents reported experiencing cyberattacks such as hacking or phishing on Instagram. This suggests that over one-third of the users are directly affected by cyber malefactions, indicating a significant risk present on the platform. Further, 61.1% of users stated they do not trust Instagram with their personal and financial information, highlighting a critical concern about data privacy and security practices on the platform.

When asked about privacy concerns, 58.3% of users admitted to avoiding some Instagram features due to fear of privacy breaches. This shows that security anxieties are impacting how users interact with the app. Despite the availability of safety tools, only 44.4% use strong passwords and 25% enable two-factor authentication, indicating a lack of widespread awareness or use of basic security measures. This demonstrates a gap in digital literacy and proactive behaviour among users.

In terms of Instagram's security efforts, 58.3% believe the platform does enough to protect users, while 36.1% disagree, showing divided confidence. Regarding fake profiles and impersonation, 36.1% of users encounter them frequently, and another 30.6% occasionally, making it a prevalent issue. Similarly, 69.4% of participants believe cyberbullying is a serious problem on Instagram, confirming that abuse and harassment are common threats.

Additionally, only 36.1% of users believe Instagram responds quickly to cybercrime reports, while others feel the response is delayed or ineffective. The presence of scams and fraudulent links was reported by 36.1% of users, showing that deceptive practices are a continuing risk. On a broader level, 86.1% of participants believe cyber threats on Instagram have increased in the past year, pointing to a rising trend of cyber malefactions.

Overall, the survey findings underscore a mismatch between the security Instagram offers and how it is perceived and used by its users. While some users take proactive steps to protect their accounts, many remain vulnerable due to insufficient knowledge or lack of confidence in the

platform's protections. These findings indicate a pressing need for better awareness, user education, and platform accountability in addressing cybercrime on Instagram.

Findings

The survey reveals that 36.1% of users have been victims of cyberattacks such as hacking or phishing, showing a considerable exposure to threats. Over 60% of respondents do not trust Instagram with personal or financial data, and a striking 86.1% believe that cyber malefactions on the platform have increased over the past year. Most users report being very concerned about data privacy (69.4%) and view cyberbullying as a serious issue. While 44.4% use strong passwords and 25% enable two-factor authentication, the varied security practices highlight inconsistent user protection behavior. Importantly, only 36.1% believe Instagram takes swift action against reports, revealing a trust deficit in the platform's responsiveness. These findings suggest a growing demand for stronger, more transparent cybersecurity policies and educational outreach by Instagram to better protect its user base.

Recommendations & Suggestion:

To mitigate cybercrime on Instagram, the following recommendations are proposed:

1. **Enhanced User Education:**
   Instagram should increase in-app tutorials and awareness campaigns about scams and safety practices.
2. **Mandatory Two-Factor Authentication for Business Accounts:**
   To protect high-risk users, two-factor authentication should be enforced by default.
3. **Stronger Content Moderation Tools:**
   Use AI to detect and remove phishing links or scam messages faster.
4. **International Cooperation on Cyber Laws:**
   Governments must work together to strengthen enforcement of cybercrime laws across borders.
5. **Report and Recovery Support:**
   Instagram should improve its support for hacked users, including faster response times and better tracking mechanisms.
6. **Partnership with Cybersecurity Firms:**
   Collaborating with external experts could help Instagram stay ahead of emerging cyber threats.

Conclusion

Cybercrime against Instagram is a growing threat that affects individuals and organizations across the globe. As Instagram continues to evolve as a social and business platform, so too do the methods of cybercriminals who exploit its features. The research confirms that while Instagram has introduced several protective measures, these are often undermined by user behaviour, lack of education, and legal complexities. Cybercrime on Instagram is not only a technological issue but also a social, legal, and educational challenge that requires a collaborative approach to combat effectively.

Reference:

1. Boyd, D., & Ellison, N. B. (2007). Social Network Sites: Definition, History, and Scholarship. Journal of Computer-Mediated Communication, 13(1), 210–230. https://doi.org/10.1111/j.1083-6101.2007.00393.x
2. Instagram Help Center. (n.d.). Privacy and Security Help. Retrieved from https://help.instagram.com/
3. https://en.m.wikipedia.org/wiki/Instagram
4. Statista. (2023). Number of Instagram users worldwide from 2019 to 2023. Retrieved from https://www.statista.com/
5. Cybercrime.gov.in. (n.d.). Report and Track Cyber Crimes in India. Ministry of Home Affairs. https://www.cybercrime.gov.in/
6. Your Google Form Survey Data. (2025). Non-doctrinal research conducted via Google Forms on Instagram cyber malefactions.
7. https//: www.researchgate.net