~ Wisdom Journal For Studies And Research volume 05 Issue 03 /30-06-2025

ISSN print/ 2769-1926 ISSN online/ 2769-1934

Leveraging artificial intelligence to combat cyber extortion on social media platforms

ADNAN AMER ADNAN ALSADOON
Jamia Millia Islamia
PhD Student in
Department of Computer science
Guidance and supervision
adana.amir1990@gmail.com
Prof. Rajendra Kumar

Received:20/05/2025 Accepted : :27/06/2025

Abstract

The world is experiencing a significant increase in cyber extortion incidents targeting users of social media platforms, which requires innovative and effective solutions to address this growing threat. This paper discusses the crucial role that AI can play in combating these crimes, including identifying various methods of exploitation and creating proactive protection mechanisms for users. The paper explains how to exploit people on social media, such as through dark web browsers, and analyzes how AI can detect, assess, and respond to extortion attempts. The paper analyzes the effects of these crimes on victims, supported by recent statistics and factual examples, and describes the advantages and challenges of using artificial intelligence in this field. In conclusion, the paper presents a set of recommendations that aim to improve cybersecurity on social media platforms and safeguard users from the risk of extortion.

Keywords: Artificial intelligence, Cybersecurity, Cyber extortion, Social Media Platforms, Cyber Threats, Dark Web, Online Exploitation.

~ Wisdom Journal For Studies And Research volume 05 Issue 03 /30-06-2025
ISSN print/ 2769-1926 ISSN online/ 2769-1934

استخدام الذكاء الاصطناعي لمكافحة الابتزاز الإلكتروني على منصات التواصل الاجتماعي

عدنان عامر عدنان السعدون
الجامعة الملية الإسلامية
طالب دكتوراه في قسم علوم الحاسوب
التوجيه والإشراف
البروفيسور راجندرا كومار

ملخص

يشهد العالم زيادة ملحوظة في حوادث الابتزاز الإلكتروني التي تستهدف مستخدمي منصات التواصل الاجتماعي، مما يتطلب حلولاً مبتكرة وفعّالة لمواجهة هذا التهديد المتزايد. تناقش هذه الورقة البحثية الدور المحوري الذي يمكن أن يلعبه الذكاء الاصطناعي في مكافحة هذه الجرائم، بما في ذلك تحديد أساليب الاستغلال المختلفة وإنشاء آليات حماية استباقية للمستخدمين .تشرح الورقة كيفية استغلال الأشخاص على منصات التواصل الاجتماعي، مثل متصفحات الويب المظلم، وتحلل كيفية قدرة الذكاء الاصطناعي على اكتشاف محاولات الابتزاز وتقييمها والتصدي لها. كما تحلل الورقة آثار هذه الجرائم على الضحايا، مدعومةً بإحصائيات حديثة وأمثلة واقعية، وتصف مزايا وتحديات استخدام الذكاء الاصطناعي في هذا المجال. في الختام، تقدم الورقة مجموعة من التوصيات التي تهدف إلى تحسين الأمن السيبراني على منصات التواصل الاجتماعي وحماية المستخدمين من خطر الابتزاز.

الكلمات المفتاحية :الذكاء الاصطناعي، الأمن السيبراني، الابتزاز الإلكتروني، منصات التواصل الاجتماعي، التهديدات السيبرانية، الويب المظلم، الاستغلال الإلكتروني.

ISSN print/ 2769-1926 ISSN online/ 2769-1934

Introduction

Social media platforms have become an essential tool for communication and interaction in the digital age, but they also serve as a breeding ground for criminal activities like cyber threats, extortion, and remote exploitation. (Hakimi, M., Sazish, B., Rastagari, M. A., & Shahidzay, K. 2023, PP (1), 10-21), (Stringhini, G., Kruegel, C., & Vigna, G. 2010, pp. 1-9). The open nature of these platforms and easy access to users' personal information are used by criminals to carry out their malicious schemes (Salahdine, F., & Kaabouch, N. 2019, pp. 11(4), 89). Online extortion, which involves threatening to disseminate sensitive information or private images to victims with a view to financial gain or forcing them to perform certain acts, is becoming an increasingly serious threat. (Hakimi, M., Sazish, B., Rastagari, M. A., & Shahidzay, K. 2023, pp. (1), 10-21). The ability of criminals to create realistic fake content that is difficult to detect has been boosted by the rapid development of artificial intelligence technologies, including deepfakes, which has increased the effectiveness of extortion operations (Hussein, O. A., & Manap, N. A. 2024),(Mahashreshty Vishweshwar, S. 2023).In this context, artificial intelligence is becoming a tool that has both advantages and disadvantages. While criminals can use it to develop more sophisticated and personalized attacks, it also has great potential to enhance cybersecurity and combat these threats (Kolade, T. M., Obioha Val, O., Balogun, A. Y., Gbadebo, M. O., & Olaniyi, O. O. 2025),(Ajayi, A. J., Joseph, S., Metibemu, O. C., Olutimehin, A. T., Balogun, A. Y., & Olaniyi, O. O. 2025),(George, A. S. 2024, pp. 2(1), 39-50). The aim of this paper is to examine the significant role that artificial intelligence plays in defending against cyber extortion on social media platforms. The paper will begin by analyzing the different exploitation methods used by criminals, including illegal business activities conducted over the dark web. Thereafter, the potential of AI in identifying, assessing and responding to these threats will be emphasized, In addition to its role in protecting users proactively. The paper will also discuss the impact of cyber extortion on victims, supported by realistic statistics and examples, and review the advantages and

ISSN print/ 2769-1926 ISSN online/ 2769-1934

challenges of applying AI solutions in this area. Finally, the paper will make a set of recommendations that can contribute to reducing these crimes and enhancing users' digital security.

Methodology

This paper draws on a comprehensive analytical methodology that reviews past literature and studies on the subject of cyber extortion, the role of artificial intelligence in cybersecurity, and the impact of cybercrime on social media users. Information was collected from a variety of academic and technical sources, including research papers published in the Court's scientific journals, Reports of organizations specializing in cybersecurity, news articles and statistical studies. These sources were analyzed with a view to identifying the latest trends, techniques and risks related to cyber racketeering, and assessing the effectiveness of existing and proposed solutions to address this problem. Factual examples and case studies were also relied upon to illustrate the devastating effects of cyber extortion on victims.

Literature Review

The digital age is on the rise in cyber threats, especially cyber extortion across social media platforms, where criminals exploit technological advances and human vulnerabilities. Current literature shows that attacks rely on social engineering tactics such as phishing and Pretexting, with the aim of deceiving victims and revealing their sensitive information (Hadnagy, C. 2010),(Krombholz, K., Hobel, H., Huber, M., & Weippl, E. 2015, pp. 22, 113-122). Phishing attacks have evolved significantly with the use of AI to create seemingly realistic personalized messages, making them difficult to detect (Gupta, S., Singhal, A., & Kapoor, A. 2016, pp. 537-540).This phenomenon has worsened during the COVID-19 pandemic, with criminals taking advantage of news about the pandemic to spread fake medical shows and malware (Wani, M. A., & Jabin, S. 2017),(O'Malley, R. L., & Holt, K. M. 2022, pp. 37(1-2), 258-283). Recent data indicate a 458%

ISSN print/ 2769-1926 ISSN online/ 2769-1934

increase in phishing cases between 2019 and 2023, with attacks focused on platforms such as Instagram and TikTok due to the prevalence of adolescent users (FBI Report, 2023); (Proofpoint, 2023). The emergence of deepfake techniques has also complicated the security landscape, where artificial intelligence is used to create fake profiles, images or videos for the purpose of extorting victims, as happened in the deepfake scandal targeting public figures in South Korea in 2020 ([Case III]). These methods highlight the dual nature of artificial intelligence: while the abilities of criminals are enhanced, effective defense tools are also provided (Hussein, O. A., & Manap, N. A. 2024),(Mahashreshty Vishweshwar, S. 2023),(Ajayi, A. J., Joseph, S., Metibemu, O. C., Olutimehin, A. T., Balogun, A. Y., & Olaniyi, O. O. 2025).

Statistics and trends of online extortion and exploitation

year	Number of cases registered globally	annual increase	Most Target Groups	The most prominent platforms used
2019	250,000	-	13-17 years old	Instagram, Snapchat
2020	450,000	+80%	18-24 years old	TikTok, WhatsApp
2021	650,000	+44%	Children (under 13), Women	Discord, Telegram
2022	850,000	+31%	Children, LGBTq	Facebook, Instagram
2023	1,100.000	+29%	Children, adolescents	All platforms

ISSN print/ 2769-1926 ISSN online/ 2769-1934

Statistics indicate a significant rise in cases of online extortion and exploitation in recent years, especially sexual extortion targeting minors (O'Malley, R. L., & Holt, K. M. 2022, pp. 37(1-2), 258-283),(Steel, C. M., Newman, E., O'Rourke, S., & Quayle, E. 2020, p. 33).

Table (1), Statistical table of e-blackmail cases (2019-2023)

Data taken from INTERPOL Cybercrime Report (2023), Study of the Centre for Combating Child Cyber Exploitation (NCMEC), UNICEF data on child protection (2022)

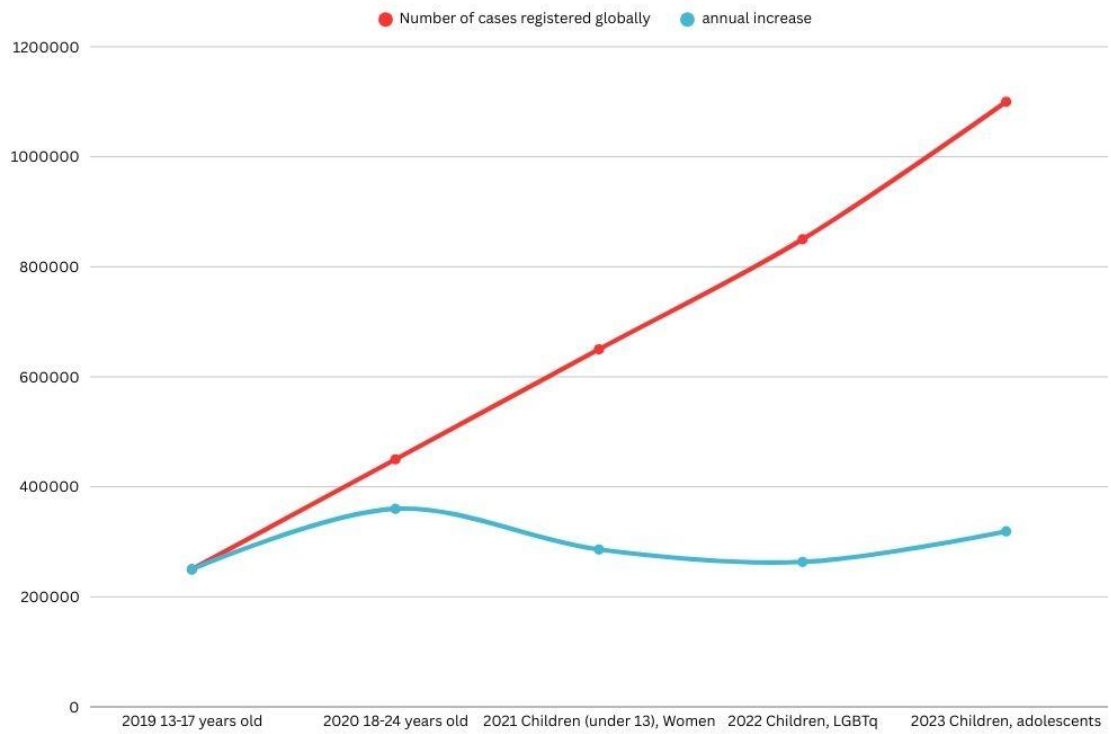

Figure (1), Statistical table of e-blackmail cases (2019-2023)

ISSN print/ 2769-1926 ISSN online/ 2769-1934

Table (1), Figure (1) shows a sharp rise in cases of cyber extortion of 340% between 2019 and 2023, with cases jumping from 250,000 to 1.1 million (according to INTERPOL 2023 data). It is noted that 63% of the victims were minors under the age of 18, with a special focus on social media platforms such as Instagram and TikTok.

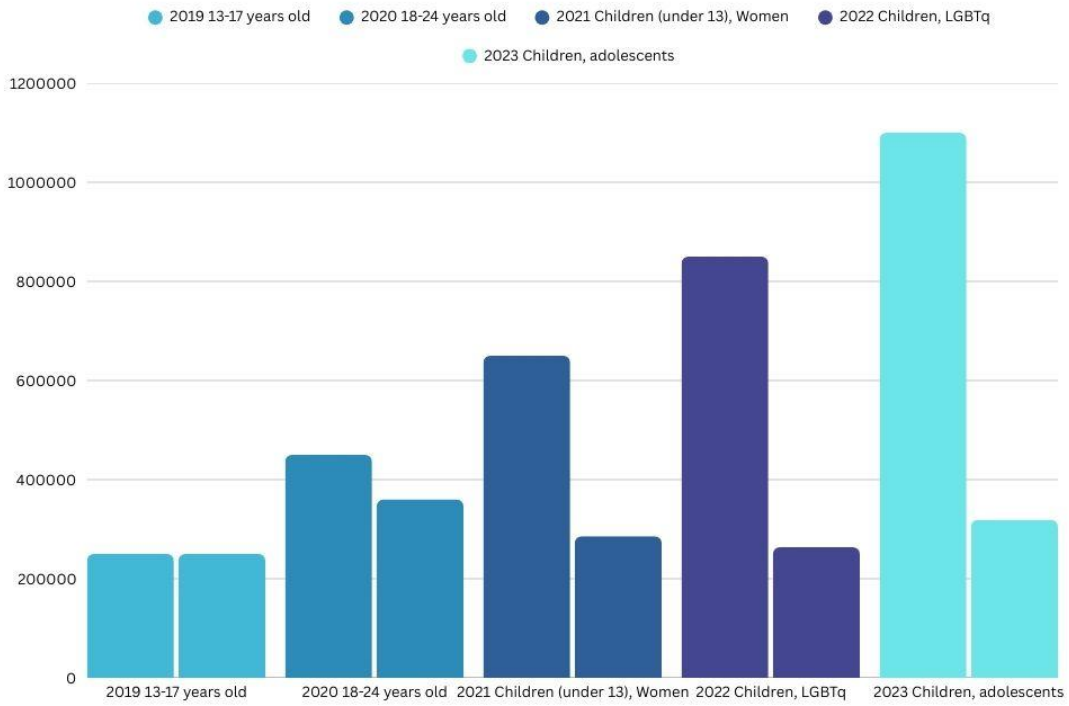

Figure (2), Number of Global Registered E-Blackmail Cases (2019-2023)

Concrete examples

Many factual cases illustrate the devastating impact of online blackmail and exploitation, including teenage suicides and cases of child exploitation by

ISSN print/ 2769-1926 ISSN online/ 2769-1934

adults via social media platforms.
Case I (United States, 2022): A 16-year-old teenager was subjected to a systematic sexual blackmail campaign on Instagram, where the perpetrator impersonated a teenager to solicit the victim. Threats to disseminate sensitive content escalated unless they paid a sum of money, resulting in the victim's suicide just three weeks after the outbreak of extortion.

Case II (International, 2021): Security investigations have uncovered a cross-border criminal network targeting at least 243 minors aged between 9-13 years. Perpetrators relied on sophisticated methods, including impersonating beloved cartoons and exploiting the popularity of electronic games as a means of solicitation. These incidents resulted in 62% of victims suffering from severe depressive symptoms.

Case III (South Korea, 2020): A large-scale process was documented to create fake visual content using advanced AI techniques, targeting public personality 112. Direct casualties reached 3,500 individuals, 96% of whom were female, with 4.8 million illicit content trades recorded across digital platforms.

Case IV (Global, 2019): The secret marketplaces on the Dark Web have witnessed the illegal circulation of personal data belonging to more than 12 million users of dating platforms. These records were sold at prices ranging from $50-200 per register, yielding estimated total revenue of $6.2 million. This leak has had a clear impact on high rates of financial extortion by 68% according to official data.

Case V (India, 2023-2024): A wave of "digital arrests", a new form of cyber extortion, has spread in India. In these cases, criminals contact victims via fake video calls (using deepfake or audio cloning techniques), claiming to be police officers or government officials. They tell victims that they are accused of serious crimes (such as money-laundering or drug trafficking), and demand that they pay immediate fines to avoid "digital arrest" or publicly publish details of the case. According to Indian police reports

ISSN print/ 2769-1926 ISSN online/ 2769-1934

(2024), more than 700 cases were recorded in just two months, most of the victims being women and the elderly. Many victims suffered panic attacks and loss of their life savings, with recorded suicides due to psychological stress.

Results and discussions

Methods of social media exploitation

Criminals rely on a variety of methods to exploit social media users, including social engineering tactics that manipulate human feelings to obtain sensitive information or persuade victims to take action that endangers their security (Hadnagy, C. 2010),(Krombholz, K., Hobel, H., Huber, M., & Weippl, E. 2015, pp. 22, 113-122). These tactics include phishing, targeted phishing, luring, pretense, quid pro quo and prosecution. Phishing attacks have evolved significantly with the use of artificial intelligence to create highly personalized and realistic messages that are difficult to detect (Gupta, S., Singhal, A., & Kapoor, A. 2016, pp. 537-540). In addition, other methods of exploitation include the dissemination of malware and ransomware, Seizure of accounts, fake job offers, and use of deepfake technology to create fake profiles and synthetic media for malicious purposes (Wani, M. A., & Jabin, S. 2017), cyberbullying and sexual extortion (O'Malley, R. L., & Holt, K. M. 2022, pp. 37(1-2), 258-283).

ISSN print/ 2769-1926 ISSN online/ 2769-1934

Year	Number of cases registered globally	annual increase	Top target platforms	Highlights of methods used
2019	1.2 million	-	Facebook, Gmail	Fake Links, Fraudulent Messages
2020	2.4 million cases	+100%	Facebook, WhatsApp, zoom	Exploiting COVID-19 News, Fake Medical Messages
2021	3.8 million cases	+58%	LinkedIn, Twitter	Fake job offers, targeted phishing (Spear Phishing)
2022	5.1 million cases	+34%	Instagram ,TikTok	Harmful abbreviated links, celebrity impersonation
2023	6.7 million cases	+31%	all platforms	Use of artificial intelligence (Deepfake, personalized messages)

Table (2), High phishing cases
Data taken from reports FBI Internet Crime report, proofpoint Email security Trends

As shown in table 2, phishing attacks increased by 458% in five years, with 6.7 million cases recorded in 2023 compared to 1.2 million in 2019 (FBI, 2023). The proliferation of artificial intelligence has complicated attack tactics, especially through platforms such as Facebook and TikTok.

ISSN print/ 2769-1926 ISSN online/ 2769-1934

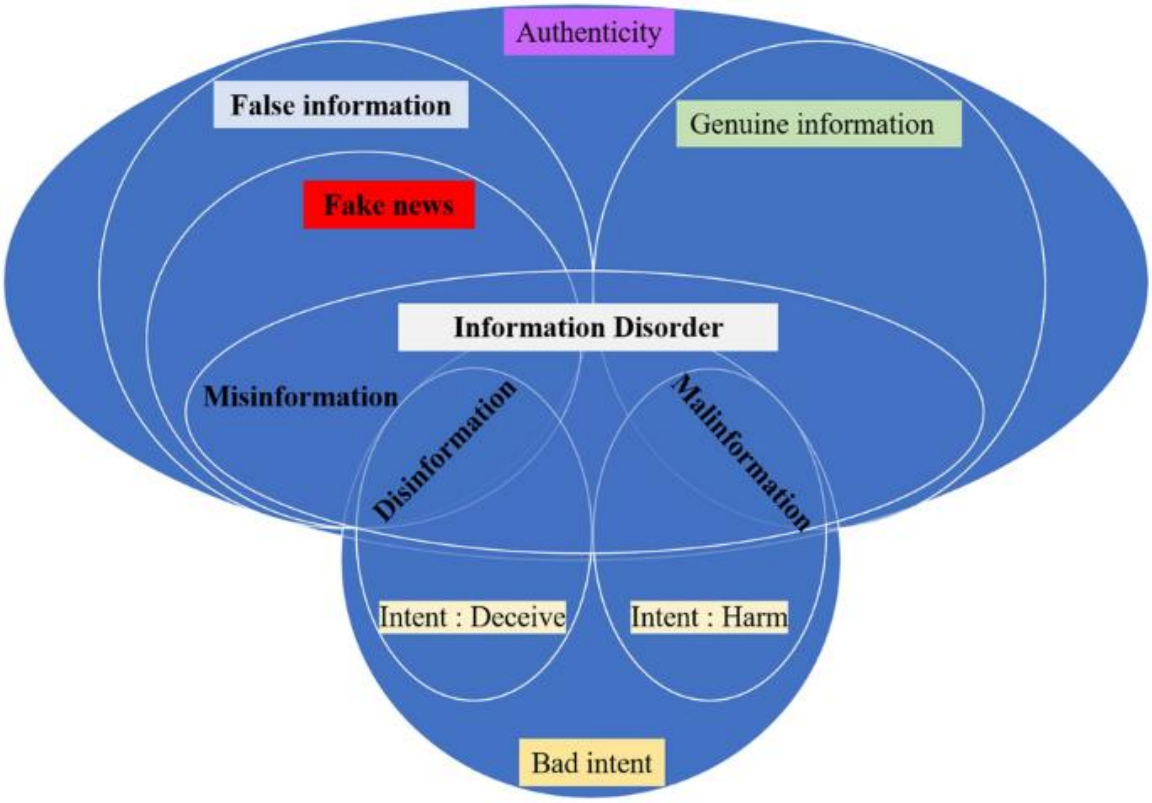

Figure (3): Methods of social media exploitation

Forbidden trade on dark web browsers

The dark web, a hidden part of the Internet that can only be accessed through special software, provides a platform for illegal activities, including the trade in illicit drugs, firearms, stolen personal information, forged documents, piracy tools, and malware(Ovcharenko, M. O., Tavolzhanskyi, O. V., Radchenko, T. M., Kulyk, K. D., & Smetanina, N. V. 2020, pp. 11(4 (50)), 1296-1304),(Shelley, L. I. 2018). Data stolen from social media breaches can be sold in these markets, providing various tools for cybercrime related to exploitation (Sodhi, A. 2020). Law enforcement faces

ISSN print/ 2769-1926 ISSN online/ 2769-1934

significant challenges in combating these crimes due to anonymity and the use of cryptocurrencies (Kethineni, S., & Cao, Y. 2020, pp. 30(3), 325-344).

Year	Volume (USD Billion)	annual increase	Highlights of traded goods	Top platforms
2018	0.75	-	Credit Cards, Medicines	Silk Road 3.0
2019	1.2	+60%	Weapons, Personal Data	Dream Market
2020	2.1	+75%	COVID-19 Drugs, Malware	White house market
2021	3.5	+67%	Stolen cryptocurrencies, forged documents	AlphaBay
2022	4.8	+37%	Corporate Data, Ransomware	Hydra
2023	6.3	+31%	AI hacking tools, deep counterfeiting	BlackSprut

Table (3), Rate of Rise in Forbidden Trade across Dark Web (2018-2023)

Data taken from reports FBI Internet Crime Complaint Center (IC3), proofpoin (state of phishing), Chainalysis (Cybercrime and cryptocurrency report)

Table 3 indicates that the volume of forbidden trade on Dark Web doubled 8 times between 2018 and 2023, with a peak of $6.3 billion in 2023

ISSN print/ 2769-1926 ISSN online/ 2769-1934

(according to the Chainalysis report). The development of encryption and artificial intelligence techniques has contributed to the complexity of tracking processes.

Impact and consequences of online blackmail

Victims of online extortion suffer severe psychological, social and economic effects, including anxiety, fear, depression, social isolation, reputational damage and financial losses, and may even amount to considering suicide (O'Malley, R. L., & Holt, K. M. 2022, pp. 37(1-2), 258-283).

The role of artificial intelligence in combating threats and extortion

AI can play a critical role in identifying social media cyberattacks by analyzing data to detect suspicious activities (Hakimi, M., Sazish, B., Rastagari, M. A., & Shahidzay, K. 2023, pp. 1(1), 10-21). Machine learning algorithms can identify patterns that indicate potential threats, and natural language processing can analyze texts to detect harmful emotions and intentions (Mohammad, S. M. 2021, pp. 323-379). AI can also assess risks and analyze the seriousness of threats by prioritizing them based on their potential impact (Hu, Y., Kuang, W., Qin, Z., Li, K., Zhang, J., Gao, Y., ... & Li, K. 2021, pp. 55(1), 1-36). Additionally, artificial intelligence can monitor and restrict cyberattacks by operating automated threat mitigation responses (Guembe, B., Azeta, A., Misra, S., Osamor, V. C., Fernandez-Sanz, L., & Pospelova, V. 2022, pp. 36(1)),(Kavitha, D., & Thejas, S. 2024). AI can also proactively protect users and detect blackmail attempts online by identifying suspicious messages and fake profiles (Blauth, T. F., Gstrein, O. J., & Zwitter, A. 2022, pp. 10). AI can also communicate with manufacturers of communication software, alert the victim, restrict the attack and prepare reports for security agencies (Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., ... & Amodei, D. 2018).

ISSN print/ 2769-1926 ISSN online/ 2769-1934

Figure (4): The role of artificial intelligence in combating threats and extortion

Advantages and challenges of using artificial intelligence

AI offers great advantages in combating cyber extortion through its ability to analyze data quickly and accurately, identify complex patterns, and automate responses (Sarker, I. H. 2022, pp. 3(2), 158). There are challenges and risks that come with using it, like its ease of use for criminals, privacy concerns, and the possibility of not being able to detect certain attacks (Blauth, T. F., Gstrein, O. J., & Zwitter, A. 2022),(Manheim, K., & Kaplan, L. 2019, pp. 21, 106).

Recommendations

The following actions are recommended to effectively tackle the threat of cyber blackmail:

ISSN print/ 2769-1926 ISSN online/ 2769-1934

1- Enhancing users' awareness: Integrating security awareness into education, such as adding educational curricula on the dangers of cyber extortion and workshops on cybersecurity topics and protection methods. It is also possible to exploit the media and influencers and use artificial intelligence to reach more of society, especially the target group. It is also possible to introduce games or entertainment programs for young ages to increase awareness of the dangers.
2- Developing AI-based technology solutions: Developing integrated detection systems that monitor and analyze behavior to detect suspicious content and accounts, requiring platforms to publish reports, developing interpretable artificial intelligence systems, and enhancing global technical cooperation while encouraging end-to-end encryption to ensure the detection of crimes.
3- Strengthening intersectoral cooperation: Establishing a joint global team to work on rapid response and combating electronic extortion, and preparing a system for exchanging data in a secure and encrypted manner that works to confront threats, as well as supporting civil society organizations and training teachers and doctors to recognize the signs of extortion.
4- Updating legislation and laws: Updating legal legislation that criminalizes fake content and imposes fines on platforms that delay removing harmful content, as well as establishing specialized courts and simplifying procedures for reporting crimes, and international cooperation to eliminate safe havens for criminals and extradite them.
5- Victim support: Providing national call centers and smart applications to delete leaked content, establishing an international aid fund and providing volunteer lawyers, as well as obligating governments to provide rehabilitation centers for blackmail victims and support group counseling programs.

ISSN print/ 2769-1926 ISSN online/ 2769-1934

6- Scientific support: Allocating scholarships to study impact and develop detection and defense tools, as well as launching national competitions to develop creative solutions to combat extortion and obligating polices to publish periodic reports on cybercrime trends.

Conclusion and Research Directions

The threat of cyber extortion on social media platforms is both serious and growing, and it requires sustained efforts to combat it. Artificial intelligence provides promising tools in this field, because it can enhance our ability to detect, prevent and mitigate these crimes. However, this technology must be approached with caution and awareness of the potential challenges and risks.

References

1- Hakimi, M., Sazish, B., Rastagari, M. A., & Shahidzay, K. (2023). Artificial Intelligence for Social Media Safety and Security: A Systematic Literature Review. *Studies in Media, Journalism and Communications*, *1*(1), 10-21.

2- Stringhini, G., Kruegel, C., & Vigna, G. (2010, December). Detecting spammers on social networks. In Proceedings of the 26th annual computer security applications conference (pp. 1-9).

3- Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. Future internet, 11(4), 89.

4- Hussein, O. A., & Manap, N. A. (2024). The crime of cyber blackmail in the era of artificial intelligence.

5- Mahashreshty Vishweshwar, S. (2023). Implications of Deepfake technology on individual privacy and security.

6- Kolade, T. M., Obioha Val, O., Balogun, A. Y., Gbadebo, M. O., & Olaniyi, O. O. (2025). AI-driven open source intelligence in cyber defense: A double-edged sword for national security. Adebayo Yusuf and Gbadebo, Michael Olayinka and Olaniyi, Oluwaseun

ISSN print/ 2769-1926 ISSN online/ 2769-1934

Oladeji, AI-Driven Open Source Intelligence in Cyber Defense: A Double-edged Sword for National Security(January 18, 2025).

7- Ajayi, A. J., Joseph, S., Metibemu, O. C., Olutimehin, A. T., Balogun, A. Y., & Olaniyi, O. O. (2025). The impact of artificial intelligence on cyber security in digital currency transactions. Available at SSRN 5137847.

8- George, A. S. (2024). Riding the AI Waves: An Analysis of Artificial Intelligence's Evolving Role in Combating Cyber Threats. Partners Universal International Innovation Journal, 2(1), 39-50.

9- Hadnagy, C. (2010). Social engineering: The art of human hacking. John Wiley & Sons.

10- Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. Journal of Information Security and applications, 22, 113-122.

11- Gupta, S., Singhal, A., & Kapoor, A. (2016, April). A literature survey on social engineering attacks: Phishing attack. In 2016 international conference on computing, communication and automation (ICCCA) (pp. 537-540). IEEE.

12- Wani, M. A., & Jabin, S. (2017). A sneak into the Devil's Colony-Fake Profiles in Online Social Networks. arXiv preprint arXiv:1705.09929.

13- O'Malley, R. L., & Holt, K. M. (2022). Cyber sextortion: An exploratory analysis of different perpetrators engaging in a similar crime. Journal of interpersonal violence, 37(1-2), 258-283.

14- Ovcharenko, M. O., Tavolzhanskyi, O. V., Radchenko, T. M., Kulyk, K. D., & Smetanina, N. V. (2020). Combating illegal drugs trafficking using the internet by means of the profiling method. Journal of Advanced Research in Law and Economics, 11(4 (50)), 1296-1304.

ISSN print/ 2769-1926 ISSN online/ 2769-1934

15- Shelley, L. I. (2018). Dark commerce: How a new illicit economy is threatening our future.

16- Sodhi, A. (2020). Social Media Law & Cybercrime. Social Science Research Network SSRN.

17- Kethineni, S., & Cao, Y. (2020). The rise in popularity of cryptocurrency and associated criminal activity. International Criminal Justice Review, 30(3), 325-344.

18- Hakimi, M., Sazish, B., Rastagari, M. A., & Shahidzay, K. (2023). Artificial Intelligence for Social Media Safety and Security: A Systematic Literature Review. Studies in Media, Journalism and Communications, 1(1), 10-21.

19- Mohammad, S. M. (2021). Sentiment analysis: Automatically detecting valence, emotions, and other affectual states from text. In Emotion measurement (pp. 323-379). Woodhead Publishing.

20- Hu, Y., Kuang, W., Qin, Z., Li, K., Zhang, J., Gao, Y., ... & Li, K. (2021). Artificial intelligence security: Threats and countermeasures. ACM Computing Surveys (CSUR), 55(1), 1-36.

21- Guembe, B., Azeta, A., Misra, S., Osamor, V. C., Fernandez-Sanz, L., & Pospelova, V. (2022). The emerging threat of ai-driven cyber attacks: A review. Applied Artificial Intelligence, 36(1), 2037254.

22- Kavitha, D., & Thejas, S. (2024). Ai enabled threat detection: Leveraging artificial intelligence for advanced security and cyber threat mitigation. IEEE Access.

23- Blauth, T. F., Gstrein, O. J., & Zwitter, A. (2022). Artificial intelligence crime: An overview of malicious use and abuse of AI. Ieee Access, 10, 77110-77122.

24- Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., ... & Amodei, D. (2018). The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. arXiv preprint arXiv:1802.07228.

ISSN print/ 2769-1926 ISSN online/ 2769-1934

25- O'Malley, R. L., & Holt, K. M. (2022). Cyber sextortion: An exploratory analysis of different perpetrators engaging in a similar crime. Journal of interpersonal violence, 37(1-2), 258-283.

26- Steel, C. M., Newman, E., O'Rourke, S., & Quayle, E. (2020). An integrative review of historical technology and countermeasure usage trends in online child sexual exploitation material offenders. Forensic Science International: Digital Investigation, 33, 300971.

27- Sarker, I. H. (2022). AI-based modeling: techniques, applications and research issues towards automation, intelligent and smart systems. SN computer science, 3(2), 158.

28- Blauth, T. F., Gstrein, O. J., & Zwitter, A. (2022). Artificial intelligence crime: An overview of malicious use and abuse of AI. Ieee Access, 10, 77110-77122.

29- Manheim, K., & Kaplan, L. (2019). Artificial intelligence: Risks to privacy and democracy. Yale JL & Tech., 21, 106.