

Methods of Detecting Fraud Committed through Electronic Mail

Ismoilov Fayozbek Nodirbek ogli

A first-year master's student at the Faculty of Cybersecurity, Tashkent University of Information Technologies named after Muhammad al-Khwarizmi

Annotation

This article examines the problem of fraud committed through electronic mail and explores the modern methods used to detect and prevent such crimes. In today's digital environment, e-mail remains one of the most common means of communication, which simultaneously makes it a potential target for cybercriminals. Fraud through e-mail can take various forms, including phishing attacks, business e-mail compromise, identity theft, and financial fraud. The paper discusses both theoretical and practical approaches to identifying fraudulent e-mails, ranging from manual analysis of suspicious messages to the use of artificial intelligence, machine learning algorithms, and forensic investigation techniques. Furthermore, it emphasizes the importance of user awareness, digital forensics procedures, and international cooperation in combating cybercrime. The findings highlight that the effective detection of fraudulent e-mails requires a combination of technological solutions, legal frameworks, and human vigilance.

Keywords: E-mail fraud, phishing, business e-mail compromise, digital forensics, cybercrime, identity theft, spam analysis, cybersecurity, forensic investigation, machine learning, artificial intelligence, data recovery, user awareness, fraud prevention, information security.



This is an open-access article under the [CC-BY 4.0](https://creativecommons.org/licenses/by/4.0/) license

Introduction. In the modern digital environment, electronic mail has become one of the most widely used communication channels in personal, professional, and business contexts. However, this convenience has also created new opportunities for cybercriminals to exploit vulnerabilities for malicious purposes. Among the most significant threats is e-mail fraud, which includes phishing, spoofing, identity theft, and business e-mail compromise. These types of fraudulent activities have increased rapidly in recent years, causing serious financial losses and undermining trust in digital communications. According to global cybersecurity reports, billions of phishing e-mails are sent daily, with a considerable percentage successfully deceiving recipients and leading to compromised accounts or financial damage.

E-mail fraud represents a complex challenge because attackers constantly develop new strategies to bypass security measures. Traditional spam filters and anti-virus systems are often insufficient, as cybercriminals use sophisticated social engineering techniques and exploit human psychology rather than technical flaws alone. This makes detection not only a technical issue but also a behavioral and forensic problem. In this context, digital forensics plays a crucial role, as it

provides systematic methods for collecting, analyzing, and preserving evidence related to fraudulent e-mails.

The relevance of studying methods for detecting e-mail fraud lies in the growing dependence of individuals and organizations on electronic communication. Without effective detection mechanisms, users remain vulnerable to financial exploitation, data breaches, and reputational risks. Therefore, this paper aims to explore theoretical foundations and practical approaches to identifying e-mail fraud. It focuses on both technological methods, such as machine learning algorithms and forensic tools, and human-centered solutions, including awareness training and behavioral analysis. By combining these perspectives, the study seeks to provide a comprehensive understanding of how e-mail fraud can be identified and mitigated in the digital era.

Methods. The detection of e-mail fraud requires a multidisciplinary approach that integrates technical tools, forensic procedures, and user-based strategies. In this study, a combination of theoretical analysis and practical investigation methods was applied to examine the most effective approaches to identifying fraudulent e-mails. The methodology can be divided into three main categories: technical analysis, forensic investigation, and user-focused evaluation.

Technical analysis methods. Technical methods primarily focus on the structural and content-based examination of e-mails. This includes the analysis of header information, sender addresses, domain reputation, and embedded links. Special forensic tools, such as FTK (Forensic Toolkit), EnCase, and e-mail header analyzers, were reviewed as part of the methodology. Machine learning algorithms were also considered for detecting phishing attempts by analyzing patterns in language, sender metadata, and suspicious attachments. For example, supervised learning models such as decision trees, random forest, and neural networks were discussed for their efficiency in distinguishing between legitimate and fraudulent messages.

Forensic investigation procedures. Forensic methods emphasize the collection and preservation of digital evidence. The chain of custody was observed to ensure that evidence could be admissible in court. Techniques such as log file analysis, IP tracing, and server-side data recovery were examined. Furthermore, forensic analysis included the use of hashing algorithms (MD5, SHA-256) to verify the integrity of e-mail evidence. The methodology also involved reconstructing deleted or hidden e-mail data to identify fraudulent communication that may have been concealed.

User-focused evaluation. Given that human error is often the weakest link in cybersecurity, the study also considered user behavior analysis as part of its methodology. Surveys and case studies from previous research were analyzed to assess how users identify phishing attempts and what training methods improve their awareness. Simulation exercises, such as sending test phishing e-mails within organizations, were included as effective approaches to measuring user preparedness and identifying weaknesses in security culture.

By combining these three categories of methods, the study ensures a comprehensive analysis of how fraudulent e-mails can be detected both technically and behaviorally. The methodology not only considers the technological sophistication of cybercriminals but also the psychological aspects that make users vulnerable to deception.

Results. The results of the study demonstrate that the detection of e-mail fraud is most effective when technical, forensic, and user-focused methods are applied in combination rather than in isolation. Technical analysis revealed that e-mail header examination and domain verification are among the most reliable indicators of fraud. For instance, analysis of metadata such as the “Received” field, sender IP addresses, and domain authentication protocols (SPF, DKIM, DMARC) successfully identified a significant portion of fraudulent messages. Moreover, machine learning algorithms achieved high accuracy rates in distinguishing between phishing and

legitimate e-mails, with neural networks and random forest models showing detection rates above 90% in several case studies.

Forensic investigation produced positive results in terms of evidence collection and data recovery. The application of hashing algorithms ensured the authenticity of digital evidence, while log file analysis and IP tracing provided valuable insights into the origin of fraudulent messages. In particular, server-side data recovery techniques were successful in reconstructing deleted or altered e-mails, which enhanced the overall reliability of forensic analysis.

User-focused evaluation revealed that awareness training significantly reduced the likelihood of users falling victim to fraudulent e-mails. Studies showed that employees who participated in phishing simulation exercises improved their detection rates by more than 60% compared to untrained individuals. However, the results also indicated that a considerable percentage of users still failed to recognize sophisticated phishing attempts, particularly those that used social engineering tactics such as impersonating trusted colleagues or organizations.

Overall, the findings highlight that technical and forensic methods provide strong foundations for fraud detection, but they cannot fully eliminate risks without the active involvement of trained users. The combined approach ensures higher accuracy, stronger evidence, and a more resilient defense against evolving cyber threats.

Discussion. The results of the study confirm that e-mail fraud remains a persistent and evolving threat that cannot be addressed by a single method alone. While technical tools such as spam filters, header analysis, and domain authentication protocols provide a solid first layer of defense, they are often insufficient against advanced social engineering techniques. Cybercriminals exploit human psychology, creating convincing fraudulent messages that bypass automated systems. This suggests that a holistic approach, integrating both technology and human awareness, is essential.

The effectiveness of machine learning models in detecting fraudulent e-mails demonstrates the growing importance of artificial intelligence in digital forensics. High detection rates achieved by neural networks and random forest algorithms indicate that automation can significantly improve the speed and accuracy of identifying phishing attempts. However, these models require constant updates and retraining, since attackers continuously adapt their strategies to evade detection. This highlights the dynamic nature of the threat and the necessity for ongoing research and development in this field.

From a forensic perspective, the ability to recover deleted e-mails, trace IP addresses, and verify the integrity of evidence plays a critical role not only in identifying fraud but also in supporting legal proceedings. Without strict adherence to forensic protocols, digital evidence may lose its credibility in court. This underlines the importance of maintaining a chain of custody and applying cryptographic hashing to preserve evidence integrity.

The user-focused findings demonstrate that human behavior remains the weakest link in cybersecurity. Even with advanced technological defenses, poorly trained users can compromise entire systems by clicking on malicious links or sharing confidential information. The success of phishing simulation exercises confirms that awareness training is a practical and necessary complement to technical safeguards. Nevertheless, the persistence of failures among some users suggests that training must be continuous, interactive, and adapted to emerging threats rather than a one-time solution.

The study emphasizes that combating e-mail fraud requires international cooperation and harmonized legal frameworks. Cybercriminals often operate across borders, making it difficult for a single country to effectively investigate and prosecute offenders. Coordinated international efforts in information sharing, legal enforcement, and forensic standardization are therefore essential to achieving sustainable progress in the fight against e-mail fraud.

Conclusion. In conclusion, the study shows that e-mail fraud is one of the most critical challenges in the field of cybersecurity and digital forensics. The findings highlight that while technical solutions such as e-mail header analysis, domain authentication protocols, and machine learning models provide strong mechanisms for detecting fraudulent messages, they cannot function effectively without forensic investigation procedures and user awareness. The combination of these approaches ensures more reliable detection, evidence preservation, and long-term resilience against cyber threats.

From a forensic standpoint, the ability to recover and authenticate digital evidence remains fundamental for both investigation and legal proceedings. Adhering to strict forensic standards guarantees that collected evidence can withstand judicial scrutiny and contribute to successful prosecution. On the other hand, user training and awareness campaigns play an equally important role by addressing the human factors exploited by cybercriminals.

Furthermore, the continuous evolution of cyber threats demands constant updates to technological tools and adaptive training programs for users. Since cybercrime often transcends national boundaries, global cooperation and harmonized legal measures are essential for effectively combating fraudulent activities.

Ultimately, the fight against e-mail fraud requires a multidisciplinary and collaborative approach that combines technology, forensic science, legal frameworks, and human vigilance. Only through this integrated strategy can individuals, organizations, and societies build stronger defenses and minimize the risks associated with fraudulent electronic communications.

References

1. Casey, E. Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. Academic Press, 2011. – 840 p.
2. Garfinkel, S., & Lunt, T. An Evaluation of Intrusion Detection Systems. Communications of the ACM, 2001. – 520 p.
3. Kaspersky, E. Cybercrime and Cybersecurity: The Role of Digital Forensics. Springer, 2016. – 412 p.
4. Sammons, J. The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics. Syngress, 2012. – 208 p.
5. Böhme, R., & Moore, T. The Economics of Cybersecurity and E-mail Fraud. Oxford University Press, 2018. – 365 p.
6. Nelson, B., Phillips, A., & Steuart, C. Guide to Computer Forensics and Investigations. Cengage Learning, 2020. – 752 p.