Business Email Compromise: A Comprehensive Taxonomy for Detection and Prevention

Amirah M Almutairi
School of Electronics and Computer Science, University of Southampton
United Kingdom
Department of Computer Science, Shaqra University
Saudi Arabia
a.almutairi@soton.ac.uk

Boojoong Kang
School of Electronics and Computer Science, University of Southampton
United Kingdom
b.kang@soton.ac.uk

Nawfal AL Hashimy
School of Electronics and Computer Science, University of Southampton
United Kingdom
nawfal@soton.ac.uk

Abstract

Business Email Compromise (BEC) is a sophisticated and increasingly prevalent form of cyber fraud that targets businesses and individuals to gain financial benefits and access sensitive data. BEC fraud involves various strategies such as impersonation, account compromise, and social engineering, making them challenging to detect and prevent. Despite numerous solutions developed to combat BEC, the threat continues to evolve. In this paper, we present a comprehensive taxonomy of BEC, categorising its various forms, detection techniques, and countermeasures. The proposed taxonomy seeks to deepen the comprehension of BEC fraud and establish a comprehensive framework for advancing research and practical applications, facilitating the development of more effective defence mechanisms against BEC fraud.

Keywords

Business Email Compromise (BEC), Taxonomy, Cyber fraud, Detection techniques, Countermeasures

ACM Reference Format:
Amirah M Almutairi, Boojoong Kang, and Nawfal AL Hashimy. 2024. Business Email Compromise: A Comprehensive Taxonomy for Detection and Prevention. In *2024 the 7th International Conference on Information Science and Systems (ICISS) (ICISS 2024), August 14–16, 2024, Edinburgh, United Kingdom.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3700706.3700714

1 Introduction

In recent years, the Internet has become an essential tool for businesses and individuals, facilitating communication, e-commerce, and various online services. However, this widespread use of online platforms has also exposed users to numerous cyber threats, among which Business Email Compromise (BEC) stands out due to its sophisticated and highly targeted nature. BEC is a form of cyber fraud that involves the use of email to deceive individuals into transferring money or divulging sensitive information. The impact of BEC is profound, leading to significant financial losses and data breaches. According to the FBI's Internet Crime Complaint Center (IC3), BEC scams caused losses exceeding USD $ 2.9 billion in 2023 alone [8]. The evolving tactics and increasing frequency of these attacks underscore the urgent need for effective detection and prevention strategies. Unlike broader phishing attacks, BEC frauds are highly personalized and often involve extensive social engineering, making them particularly challenging to detect. Taxonomy is a structured, objective methodology for categorizing diverse criteria into distinct classes. The efficacy of a taxonomy hinges on its capacity to comprehensively represent the entirety of the object and to offer a precise and coherent description and presentation. Given the complexity and high stakes associated with BEC, there is a critical need for a structured taxonomy to classify and understand the various forms of these attacks. A well-defined taxonomy can serve as a common reference for both academia and industry, providing clarity and aiding in the development of robust defence mechanisms. Business Email Compromise (BEC) is a growing and sophisticated form of cyber fraud that targets businesses and individuals to gain financial benefits and access to sensitive data. BEC attacks typically involve strategies such as impersonation, account compromise, and social engineering, making them particularly challenging to detect and prevent. The increasing prevalence of BEC has resulted in significant financial losses and data breaches worldwide. The evolution of BEC tactics and the adaptability of attackers highlight the urgent need for robust detection and prevention mechanisms. Despite numerous solutions developed to combat BEC, the threat continues to evolve, adapting to new technologies and exploiting human vulnerabilities. Existing literature has explored various aspects of BEC and phishing, but a comprehensive taxonomy specifically tailored to BEC is still lacking. Such a taxonomy is crucial for systematically categorizing BEC incidents, understanding their various forms, and developing effective countermeasures.

The **objectives** of this paper are to:

- Present a comprehensive taxonomy of BEC, categorizing its various forms, methodologies, targets, countermeasures, and challenges.
- Improve understanding of BEC attacks to support the development of more effective detection and prevention mechanisms.
- Establish a detailed framework for future research and practical applications in combating BEC.

ICISS 2024, August 14–16, 2024, Edinburgh, United Kingdom

ACM ISBN 979-8-4007-1756-7/24/08
https://doi.org/10.1145/3700706.3700714

This paper is the first to present a comprehensive taxonomy of BEC, categorizing BEC based on their anatomy, methodologies, targets, countermeasures, and challenges. By doing so, it **aims** to fill this significant gap in the literature, providing a clearer understanding of BEC and supporting the development of more effective detection and prevention mechanisms tailored to this particular threat.

The structure of this paper is as follows: **Section 1** provides an introduction to Business Email Compromise (BEC), highlighting the objectives and aims of the study. **Section 2** reviews the related work on BEC fraud. **Section 3** introduces the proposed taxonomy of BEC fraud. **Section 4** validates the taxonomy through literature review and case studies. Finally, **Section 5** summarizes the study's findings and provides recommendations for future research.

2 Related Works

The literature on Business Email Compromise (BEC) is vast, with numerous studies exploring various aspects of these cyber threats. However, a closer examination of recent literature reviews reveals certain limitations that underscore the need for a more comprehensive taxonomy specifically tailored to BEC. Papathanasiou et al. [16] primarily focused on the landscape of BEC fraud in Greece and examined the regulatory framework under the EU's NIS Directives. Their study provided valuable perspectives on the effectiveness of countermeasures within this region and offered recommendations for enhancing cybersecurity practices. However, the findings and recommendations were largely region-specific and did not capture the global diversity of BEC fraud vectors and responses. This limits the generalizability of their insights to other regions and contexts. Furthermore, Ogwo-Ude [15] conducted an in-depth examination of BEC fraud and its significant financial impact, particularly focusing on the challenges faced by small and medium-sized enterprises (SMEs) in the United States. While this study offered tailored mitigation strategies for smaller organizations, it did not fully address the unique circumstances and requirements of larger organizations or different sectors. The findings were specific to SMEs in the USA, indicating a need for broader research that encompasses various organizational contexts to effectively mitigate BEC risks. Additionally, Atlam and Oluwatimilehin [2] provided a comprehensive overview of phishing detection techniques, addressing a broad spectrum of attacks including spear phishing, general phishing, and BEC. Although their review covered a wide range of phishing-related topics, the findings and recommendations were not entirely specific to BEC. Their work highlighted the necessity for additional research focused exclusively on BEC fraud to develop targeted detection strategies that can supplement the existing insights on phishing. Despite the numerous research on BEC and related cyber threats, there remains a gap in comprehensive taxonomies that are specifically designed for BEC. None of the existing studies have developed a taxonomy that categorizes BEC attacks in a structured manner.

3 The Proposed Taxonomy

The taxonomy presented in **Figure 1** offers a structured classification of BEC attacks, encompassing their anatomy, methodologies, targets, countermeasures, and associated challenges. By providing a comprehensive overview, this taxonomy highlights key areas for further investigation and development. It serves as a foundation for researchers and practitioners to formulate more resilient strategies to mitigate BEC fraud. The components of the proposed taxonomy are delineated as follows:

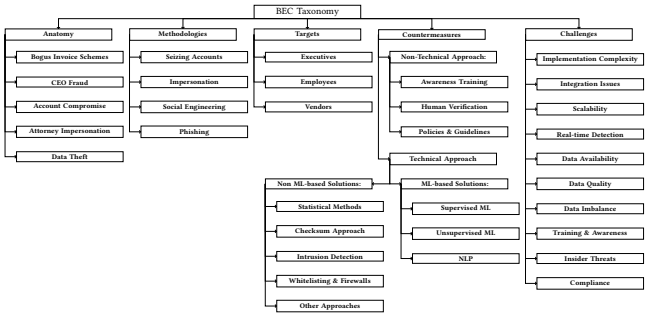

Figure 1: Classification of BEC by anatomy, methodologies, targets, countermeasures, and challenges, providing a comprehensive taxonomy.

3.1 Classify by Anatomy

Business Email Compromise (BEC) attacks can take on various forms, each with distinct characteristics and tactics. Key forms of BEC include:

- **Bogus Invoice Schemes:** Attackers impersonate vendors or suppliers and send fraudulent invoices to businesses, tricking them into making payments to fraudulent accounts.
- **CEO Fraud (Executive Impersonation):** Attackers pose as high-ranking executives (e.g., CEO or CFO) and request urgent wire transfers or sensitive information from employees.
- **Account Compromise:** Attackers gain access to a legitimate business email account and use it to conduct unauthorized transactions or send phishing emails.
- **Attorney Impersonation:** Attackers impersonate lawyers or legal representatives and request confidential information or payments, often under the guise of legal urgency.
- **Data Theft:** Attackers seek to obtain sensitive data, such as employee personal information or customer records, which can be used for further fraud or sold on the black market.

Understanding these various forms is crucial for developing tailored detection and prevention strategies.

3.2 Classify by Methodologies

BEC attackers employ a range of methods to execute their schemes. The most common methodologies include:

- **Seizing Accounts:** Attackers gain unauthorized access to business email accounts through phishing, malware, or brute force attacks. Once inside, they can monitor communications and manipulate email threads to perpetrate fraud.
- **Impersonation:** Attackers use spoofed email addresses or compromised accounts to pose as trusted individuals, such as executives, employees, or business partners, to deceive their targets.

- **Social Engineering:** Attackers exploit human psychology to trick individuals into divulging confidential information or performing actions that facilitate the attack. Techniques include pretexting, baiting, and creating a sense of urgency.
- **Phishing:** Cybercriminals send seemingly authentic emails to deceive recipients into clicking on malicious links, downloading harmful software, or disclosing confidential information.

These methodologies are often used in combination to increase the likelihood of a successful attack.

3.3 Classify by Targets

BEC attacks can be directed at various targets within an organization, including:

- **Executives:** High-ranking officials with decision-making power and access to sensitive information.
- **Employees:** Staff members, particularly those in finance or administrative roles, who handle transactions and sensitive data.
- **Vendors and Partners:** External entities that have a business relationship with the organization may be impersonated or compromised to facilitate BEC attacks.

3.4 Classify by Countermeasures

Countermeasures can be categorized into technical and non-technical approaches:

Classify by Technical Approach:

- **Non ML-based Solutions:** Includes statistical methods, checksum approach, intrusion detection methods, and whitelisting and firewall methods.
- **ML-based Solutions:** Includes supervised ML, unsupervised ML, and NLP techniques.

Classify by Non-Technical Approach:

- **Awareness Training:** Training employees to recognize and respond to BEC threats.
- **Human Verification:** Implementing verification steps to confirm the legitimacy of requests.
- **Policies and Guidelines:** Establishing clear policies and guidelines to prevent BEC attacks.

3.5 Classify by Challenges

Despite numerous solutions suggested in the literature for detecting BEC attacks, a definitive solution to counteract these threats remains elusive. The persistence and evolution of BEC fraud continue to pose significant challenges, establishing it as one of the most prevalent forms of cybercrime today. Many of the proposed solutions may prove inadequate or insufficient in addressing the intricate complexities of BEC.

3.5.1 Challenges in Technical Solutions. Technical solutions for detecting BEC can be broadly categorized into non-ML-based and ML-based solutions, each facing unique challenges.

Challenges in Non-ML-Based Solutions. Non-ML-based solutions typically involve filtering methods that use specific word combinations to identify suspicious emails. The challenges include:

- **Implementation Complexity:** Developing and maintaining effective non-ML-based filters require significant effort and expertise to ensure they can handle the sophisticated and evolving nature of BEC attacks.
- **Integration Issues:** Integrating these filters with existing email systems and ensuring they do not disrupt regular communication can be challenging.
- **Scalability:** As organizations grow, the email volume increases, and ensuring that filtering systems scale efficiently without compromising performance is essential.
- **Real-time Detection:** Non-ML-based filters may struggle to provide real-time detection and response, which is critical for preventing immediate financial losses or data breaches.

Challenges in ML-Based Solutions. ML-based solutions use Natural Language Processing (NLP) and machine learning techniques. The challenges include:

- **Data Availability:** Significant amounts of labelled data are required to train effective ML models, which can be difficult to obtain due to privacy concerns and the scarcity of publicly available datasets.
- **Data Quality:** The quality of training data directly impacts the model's effectiveness. Poor-quality data can lead to inaccurate models that fail to detect sophisticated BEC attacks.
- **Data Imbalance:** BEC datasets often have an imbalance between legitimate emails and fraudulent ones, which can skew model training and reduce detection accuracy.
- **Contextual Understanding:** Existing ML approaches might not adequately consider the semantic context or the subtleties of language used in BEC scams, leading to potential misclassifications [5, 7].

3.5.2 Challenges in Non-Technical Solutions. Non-technical solutions are equally vital in combating BEC but face several hurdles, primarily related to human factors and organizational behaviour.

Training and Awareness. The effectiveness of BEC detection heavily relies on human intelligence and behaviour. The challenges include:

- **Training and Awareness:** Employees may inadvertently bypass security protocols due to a lack of awareness or understanding of BEC threats. Continuous and up-to-date training programs are necessary but can face resistance from employees.
- **Insider Threats:** Employees with access to sensitive information can be manipulated or may willingly participate in fraudulent activities. Detecting and preventing insider threats requires robust monitoring and response strategies.

Organizational Culture and Compliance. The overall culture and policies of an organization significantly impact the success of non-technical measures. The challenges include:

- **Compliance:** Organizations must comply with various regulatory requirements related to data security and privacy. Ensuring compliance while implementing BEC detection measures can be complex, as it involves navigating different legal frameworks and standards.

- **Security Prioritization:** In environments where security is not prioritized, employees are less likely to follow stringent security practices. Balancing security with operational efficiency is crucial, as overly stringent measures can hinder business processes, while lax policies can leave the organization vulnerable.

Addressing the challenges of BEC prevention requires a multifaceted approach that combines technical and non-technical solutions. Both human and technological factors must be considered to develop effective strategies against this persistent threat.

4 Validation of the Proposed Taxonomy

In evaluating the quality of a taxonomy, two critical factors are its level of detail and its adaptability. Consequently, we assessed our proposed taxonomy for BEC attacks by examining its performance and how it influences the notation of BEC phishing attacks. To validate the proposed taxonomy, we employed a multi-faceted approach that included a thorough literature review and case study analysis.

4.1 Literature Review

To validate the proposed taxonomy, a comprehensive literature review was conducted. This review aimed to ensure the completeness and accuracy of the taxonomy by cross-referencing its components with existing research on Business Email Compromise (BEC). The literature review involved the following steps:

4.1.1 Selection of Sources. A variety of sources were selected, including academic papers, industry reports, and white papers. Key databases such as IEEE Xplore, Google Scholar, and Web of Science were used to search for relevant studies. Keywords such as "Business Email Compromise," "BEC fraud" and "BEC countermeasures" were employed to identify pertinent literature.

4.1.2 Analysis of Literature. The selected studies were analyzed to identify the key components of BEC attacks, detection techniques, countermeasures, and challenges. The findings from these studies were then mapped to the categories defined in our taxonomy.

Non-Technical Solutions. Several studies confirm the importance of non-technical solutions in combating BEC fraud. We can classify these studies into three main categories: awareness training, human verification, and policies. Awareness training is critical for educating employees about phishing and BEC fraud. For instance, Mansfield-Devine [12] and Binks [3] highlight the role of awareness training in helping employees recognize and respond to phishing attempts. Human verification involves practical approaches to mitigate risks. The FBI [6] and Meyers [13] suggest methods such as implementing multiple sign-offs on significant transactions and requiring human verification to ensure the authenticity of emails and transactions. Policies provide a structured framework to prevent BEC fraud. Ross [17] and Zweighaft [22] discuss the effectiveness of simulated assault training and comprehensive training programs, while Burns et al. [4] proposes establishing a business governance framework for high-value email transactions. These policies add layers of verification and establish protocols to prevent fraudulent activities. These non-technical measures align well with the "Non-Technical Approach" section of our taxonomy.

Technical Solutions. Technical solutions for BEC detection can be divided into Non-ML-based and ML-based categories.

`Non-ML-based Solutions:` Several studies have focused on non-ML-based solutions, highlighting the practicality of methods such as checksum and intrusion detection systems. Teerakanok et al.[19] describe a method using checksum to verify the authenticity of invoices, offering a solid defence against bogus invoice schemes. Additionally, Sahoo and Rajitha [18] propose an intrusion detection strategy to distinguish fake emails from legitimate ones, providing an effective non-ML-based solution for BEC detection.

`ML-based Solutions:` Machine learning and natural language processing (NLP) techniques have been extensively applied to BEC detection. Maleki [11] employs K-means clustering and sentiment analysis to identify BEC emails, showcasing the potential of clustering techniques in cybersecurity. Cidon et al.[5] propose a two-stage ML approach that integrates metadata and textual analysis for real-time BEC detection, confirming the importance of multi-source data integration. Vorobeva et al.[21] using NLP techniques, such as TF-IDF and k-means clustering, to detect BEC patterns, demonstrating the effectiveness of NLP in identifying fraudulent emails. Almutairi et al.[1] introduce a transformer-based method combining BERT and BiLSTM, focusing on the linguistic properties of emails to detect BEC attacks with high accuracy. Their approach outperforms state-of-the-art solutions, achieving a detection accuracy of 99%. These studies collectively support the technical approaches outlined in our taxonomy, highlighting the effectiveness of both ML-based and non-ML-based solutions in combating BEC fraud.

Challenges. Several studies have identified significant challenges in combating Business Email Compromise (BEC). Real-time detection remains a formidable challenge, necessitating robust and adaptive systems capable of responding to rapidly evolving threats. The availability, quality, and imbalance of data are critical factors that significantly influence the effectiveness of BEC detection methods [1]. High-quality, comprehensive datasets are essential for training effective machine learning models, yet such datasets are often scarce due to privacy concerns and the proprietary nature of corporate data. In addition to technical hurdles, the human element introduces further challenges. Effective BEC mitigation requires ongoing training and awareness programs to educate employees about potential threats. However, insider threats—where employees may intentionally or unintentionally compromise security—and varying levels of compliance across organizations complicate these efforts. Nehme and George [14] and Lazarus [10] discuss how these human factors, combined with organizational culture and behaviour, play a crucial role in the overall security posture against BEC attacks. Overall, addressing the challenges associated with BEC requires a multi-faceted approach that integrates advanced technical solutions with comprehensive human-centric strategies. Ensuring the seamless interplay between technology and human vigilance is vital to enhancing organizational resilience against BEC threats.

The literature review confirms the comprehensiveness and accuracy of the proposed taxonomy. By aligning existing research findings with the taxonomy's components, we have shown that it is well-founded in current BEC knowledge. This validation ensures the taxonomy's robustness and reliability for guiding future research and practical applications in combating BEC fraud.

4.2 Case Study 1: Treasure Island Homeless Charity

This case study evaluates the effectiveness of our proposed BEC taxonomy in analyzing a real-world incident involving Treasure Island Homeless Charity [20]. The study aims to demonstrate the taxonomy's applicability, effectiveness in categorization, and its role in understanding BEC incidents.

4.2.1 Case Study Overview. In June 2021, Treasure Island, a San Francisco-based homelessness charity, fell victim to a severe BEC attack resulting in a loss of $625,000. Over the course of a month, cybercriminals infiltrated the organization's bookkeeper's email system. They exploited this access to manipulate a legitimate invoice from one of Treasure Island's partner organizations. Consequently, the charity inadvertently transferred funds intended for the partner directly into the hackers' bank account.

4.2.2 Application of the Taxonomy. Using our proposed BEC taxonomy, we categorized the incident as follows:

- **Anatomy:** The attack involved email infiltration and manipulation of financial transactions via a bogus invoice.
- **Detection Techniques:** The attack went undetected until after the funds were transferred, highlighting deficiencies in anomaly detection systems.
- **Countermeasures:** Post-incident recommendations include implementing multi-factor authentication (MFA), enhancing email security training, instituting robust verification processes for financial transactions, and acquiring cybercrime insurance.
- **Challenges:** Challenges included sophisticated manipulation of invoices, delayed detection, and the nonprofit sector's limited cybersecurity resources.

4.3 Case Study 2: Insurance Broker Firm

This case study assesses the application of our proposed BEC taxonomy in a real-world scenario involving an insurance broker firm [9]. The aim is to illustrate the taxonomy's effectiveness in categorizing BEC incidents and enhancing understanding and prevention strategies.

4.3.1 Case Study Overview. As a specialist firm providing insurance advice for high-value business mergers and acquisitions, Kroll's client processes a wealth of sensitive data. Despite maintaining high security, the firm discovered it had been compromised by a cybercriminal and used it as a platform to launch a BEC attack aimed at tricking one of its clients into paying nearly £300,000 into an alternate bank account. The attack was detected before any payment was made. Kroll conducted a forensic investigation, revealing that the attack began with a successful phishing attempt six weeks prior [9].

4.3.2 Application of the Taxonomy. Using our proposed taxonomy, we categorized the incident as follows:

- **Anatomy:** The attack began with a phishing email, leading to email rule manipulation and spoofing to trick the client into making a payment.
- **Detection Techniques:** The vigilant verification process by the client's staff and the forensic investigation by Kroll helped detect the attack before any financial loss occurred.
- **Countermeasures:** Post-incident, the insurance broker implemented MFA, locked down compromised accounts, and enforced security protocols as recommended by Kroll.
- **Challenges:** The primary challenges included sophisticated phishing tactics, convincing spoof emails, and continuous efforts by attackers to conceal their actions.

4.4 Results

The efficacy of the proposed taxonomy is confirmed through a comprehensive literature review and case studies, which validate its comprehensiveness and accuracy. By mapping the findings from existing research to the taxonomy's components, we have demonstrated that the taxonomy is grounded in the current body of knowledge on BEC. This validation step ensures that the taxonomy is robust and reliable for guiding future research and practical applications in combating BEC fraud.

Furthermore, The application of our proposed BEC taxonomy to both case studies; Treasure Island Homeless Charity and the insurance broker firm—effectively categorized the elements of these BEC incidents. The taxonomy provided a structured framework for understanding the attack's anatomy, the detection challenges encountered, the countermeasures employed, and the specific challenges faced by different sectors. In the case of Treasure Island Homeless Charity, the taxonomy helped to systematically categorize the incident involving email infiltration and manipulation of financial transactions via bogus invoices. The charity experienced a significant financial loss due to the attack, but the taxonomy facilitated a detailed analysis of the attack's anatomy, detection challenges, countermeasures, and sector-specific challenges. This included recommendations for multi-factor authentication (MFA), enhanced email security training, robust verification processes for financial transactions, and cybercrime insurance. The charity also faced challenges due to limited cybersecurity resources in the nonprofit sector. For the insurance broker firm, the taxonomy was applied to analyze a BEC incident where phishing emails led to rule manipulation and unauthorized wire transfers. The structured categorization provided insights into the attack's anatomy, detection challenges, countermeasures, and sector-specific challenges. This included implementing advanced email filtering, regular security audits, and employee training on recognizing phishing attempts, while addressing the high value of transactions and the necessity for strict compliance with regulatory standards.

Overall, the taxonomy systematically categorized the incidents, offering clear insights into the attack methods, such as email infiltration, manipulation of financial transactions, and phishing emails leading to rule manipulation. This structured categorization underscored the taxonomy's practical relevance and utility in real-world scenarios, highlighting critical areas for improvement in BEC prevention and response strategies. By applying the proposed taxonomy, both organizations were able to develop more structured and comprehensive approaches to detecting and preventing BEC attacks, enhancing their overall resilience against such threats.

5 Conclusion

Business Email Compromise (BEC) represents a sophisticated form of cyber fraud that poses significant risks to both businesses and individuals, often resulting in substantial financial losses and data breaches. This paper introduced a comprehensive taxonomy designed to improve the understanding, detection, and countering of BEC attacks. By classifying BEC incidents based on their anatomy, methods, strategies, targets, countermeasures, and associated challenges, the taxonomy provides a detailed and structured framework. The proposed taxonomy offers a clear and structured reference that strengthens both academic and practical approaches to combating BEC. Its validation through literature review and case studies underscores its applicability and relevance in real-world scenarios, demonstrating its potential as a reliable framework for further research and practical applications. By systematically reviewing existing literature, this study clarifies the terminology associated with BEC and guides future research and practical implementations. The findings from this taxonomy can be utilized to develop more effective defense mechanisms against the evolving threat of BEC, ultimately contributing to improved cybersecurity practices. Future research should focus on advancing detection techniques and preventive measures, integrating the taxonomy into existing cybersecurity frameworks to bolster organizational resilience against BEC threats. This taxonomy serves as a foundational tool for researchers, practitioners, and policymakers, facilitating a better understanding and mitigation of the risks associated with BEC. By contributing to the broader effort of securing digital communications and protecting sensitive information, this taxonomy plays a crucial role in enhancing overall cybersecurity.

References

[1] Amirah Almutairi, BooJoong Kang, and Nawfal Fadhel. 2023. The Effectiveness of Transformer-Based Models for BEC Attack Detection. In *International Conference on Network and System Security*. Springer, 77–90.

[2] Hany F. Atlam and Olayonu Oluwatimilehin. 2022. Business Email Compromise Phishing Detection Based on Machine Learning: A Systematic Literature Review. *Electronics* null (2022), null. https://doi.org/10.3390/electronics12010042

[3] Adam Binks. 2019. The art of phishing: past, present and future. *Computer Fraud & Security* 2019, 4 (2019), 9–11.

[4] AJ Burns, M Eric Johnson, and Deanna D Caputo. 2019. Spear phishing in a barrel: Insights from a targeted phishing campaign. *Journal of Organizational Computing and Electronic Commerce* 29, 1 (2019), 24–39.

[5] Asaf Cidon, Lior Gavish, Itay Bleier, Nadia Korshun, Marco Schweighauser, and Alexey Tsitkin. 2019. High precision detection of business email compromise. In *28th USENIX Security Symposium (USENIX Security 19)*. 1291–1307.

[6] FBI. 2021. Operation rewired. https://www.ic3.gov/Media/Y2022/PSA220504

[7] Hugo Gascon, Steffen Ullrich, Benjamin Stritter, and Konrad Rieck. 2018. Reading between the lines: content-agnostic detection of spear-phishing emails. In *International Symposium on Research in Attacks, Intrusions, and Defenses*. Springer, 69–91.

[8] Internet Crime Complaint Center. 2023. 2023 Internet Crime Report. https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf Accessed: 2024-05-24.

[9] Kroll. 2021. Business Email Compromise Attack Investigation and Remediation for Insurance Broker. https://www.kroll.com/en/insights/publications/cyber/case-studies/business-email-compromise-attack-investigation Accessed: 2024-06-05.

[10] Suleman Lazarus. 2024. Cybercriminal Networks and Operational Dynamics of Business Email Compromise (BEC) Scammers: Insights from the "Black Axe" Confraternity. *Deviant Behavior* (2024), 1–25.

[11] Nasim Maleki. 2019. *A behavioral based detection approach for business email compromises*. Ph. D. Dissertation. University of New Brunswick.

[12] Steve Mansfield-Devine. 2016. The imitation game: How business email compromise scams are robbing organisations. *Computer Fraud & Security* 2016, 11 (2016), 5–10.

[13] Adam Meyers. 2018. Not your fairy-tale prince: the Nigerian business email compromise threat. *Computer Fraud & Security* 2018, 8 (2018), 14–16.

[14] Alaa Nehme and Joey F George. 2018. Iterating the cybernetic loops in anti-phishing behavior: A theoretical integration. *Twenty-fourth Americas Conference on Information Systems* (2018).

[15] Okechukwu Ogwo-Ude. 2023. Business email compromise challenges to medium and large-scale firms in USA: An Analysis. *Open Journal of Applied Sciences* 13, 6 (2023), 803–812.

[16] Anastasios Papathanasiou, George Liontos, Vasiliki Liagkou, and Euripidis Glavas. 2023. Business Email Compromise (BEC) Attacks: Threats, Vulnerabilities and Countermeasures—A Perspective on the Greek Landscape. *Journal of Cybersecurity and Privacy* 3, 3 (2023), 610–637.

[17] Chris Ross. 2018. The latest attacks and how to stop them. *Computer Fraud & Security* 2018, 11 (2018), 11–14.

[18] Prasanta Kumar Sahoo and Cheguri Rajitha. 2019. Detecting Forged E-Mail using Data Mining Techniques. *International Journal of Engineering and Advanced Technology* (2019).

[19] Songpon Teerakanok, Hiroaki Yasuki, and Tetsutaro Uehara. 2020. A Practical Solution against Business Email Compromise (BEC) Attack using Invoice Checksum. *Proceedings - Companion of the 2020 IEEE 20th International Conference on Software Quality, Reliability, and Security, QRS-C 2020* (2020), 160–167. https://doi.org/10.1109/QRS-C51114.2020.00036

[20] Tessian. 2021. Business Email Compromise Examples. https://www.tessian.com/blog/business-email-compromise-bec-examples/ Accessed: 2024-06-05.

[21] Alisa Vorobeva, Guldar Khisaeva, Danil Zakoldaev, and Igor Kotenko. 2021. Detection of Business Email Compromise Attacks with Writing Style Analysis. In *International Symposium on Mobile Internet Security*. Springer, 248–262.

[22] David Zweighaft. 2017. Business email compromise and executive impersonation: are financial institutions exposed? *Journal of Investment Compliance* (2017).