Business Email Compromise Defender

Subjects: Others

Contributor: Anastasios Papathanasiou , George Liontos , Georgios Paparis , Vasiliki Liagkou , Euripides Glavas

In an era of ever-evolving and increasingly sophisticated cyber threats, protecting sensitive information from cyberattacks such as business email compromise (BEC) attacks has become a top priority for individuals and enterprises. According to the available literature, various authentication methods have been explored for validating physical documents using QR codes.

business email compromise (BEC) email security QR code encryption cryptography

1. Introduction

Email has become an integral part of our daily lives, with over 333.2 billion emails sent and received per day in 2022 worldwide [1]. However, the convenience of email has also led to an increase in cyberattacks, including business email compromise (BEC) attacks. In a BEC attack, an attacker impersonates a legitimate sender to deceive the receiver into sending money or sensitive information.

More specifically, in a typical business email compromise (BEC) scheme, the perpetrators carefully select their target and employ a series of tactics to gather valuable information from open-source intelligence (OSINT) techniques [2] and then construct an elaborated malicious email, often assuming the identity of a trusted entity or source. Within this fraudulent email, the attacker may employ sophisticated social engineering techniques, designed to manipulate and coerce the recipient into taking actions that ultimately benefit the scammer. Alternatively, the email may include malicious payloads, such as viruses concealed in various attachments or deceitful links. These malicious actions serve multiple nefarious purposes. Firstly, they aim to compromise the victim's communication channels, potentially allowing the scammer to intercept sensitive information. Moreover, the attacker may seek to extract money or valuable data from the unsuspecting victim [3][4]. In essence, BEC attacks represent a multifaceted threat that combines careful target selection, information gathering, persuasive impersonation, and the deployment of harmful software or links to achieve illegal objectives.

These attacks are often successful because they exploit human error, such as trusting an email's contents without verifying its authenticity. In 2022 alone, BEC attacks resulted in losses of nearly USD 2.7 billion globally, which is an escalation of approximately USD 350 million from the preceding year (2021), and a notable surge of around USD 860 million from the year 2020, according to the FBI statistics report [5].

Figure 1 depicts a general BEC scheme timeline. In Step 1, the attackers identify a target, most commonly a CEO or CFO. The primary objective of the attacker is to extract financial gains or confidential data by assuming the

identity of a high-ranking individual within a corporation. However, the final or intermediary victims can range from the CEO or CFO to employees within different departments, such as accountants or IT personnel. In Step 2, the attackers employ social engineering techniques in order to gather information about the victim or victims (employees or associates in the targeting enterprise), and, in Step 3, the attacker crafts a sophisticated email in order to extract funds or intercept sensitive information (Step 4) [6].

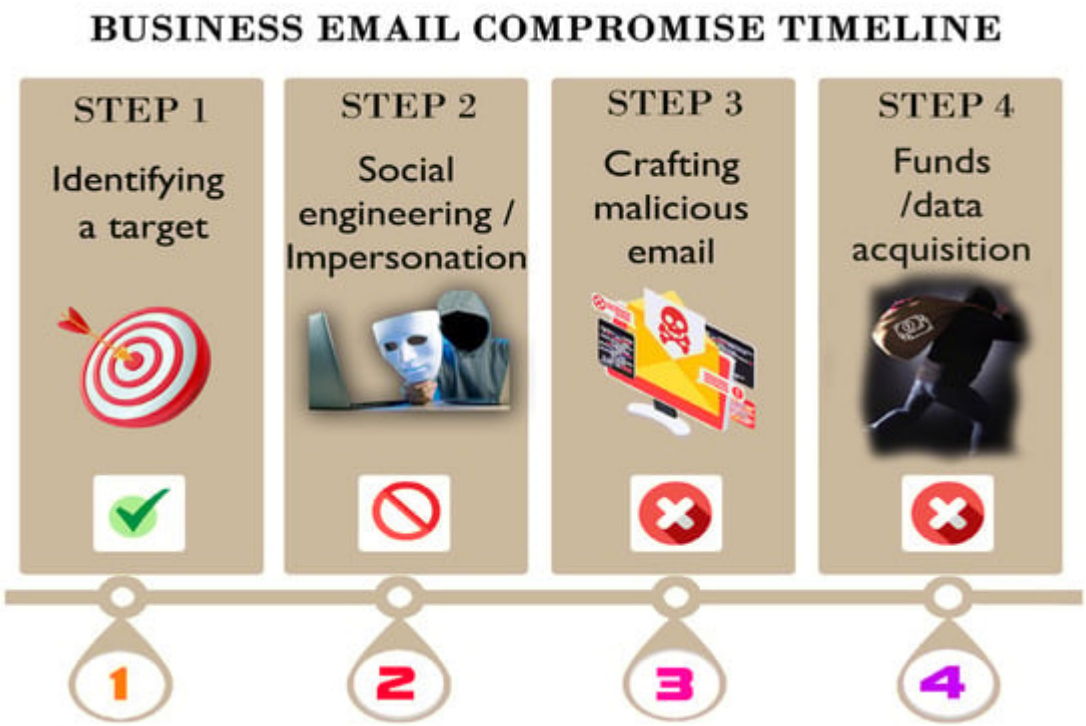

Figure 1. Business email compromise timeline.

2. QR Codes in Hard Copies for Document Authentication

According to the available literature, various authentication methods have been explored for validating physical documents using QR codes, as discussed in the subsequent Sections. The incorporation of QR code solutions in these academic works demonstrates promise in the realm of verifying the authenticity of hard-copy documents through the scanning of the QR code by an authentication device. It is worth noting that these methods primarily refer to physical documents and may not be applicable to email communications for countering business email compromise (BEC) attacks.

Singhal A et al. [7] propose a method that verifies a university degree certificate with the use of a QR code that contains a digital signature over the data, such as the degree holder's name, enrollee number, roll number, etc. To achieve the same objective, Aini Q. et al. [8] propose a method for authenticating a university diploma by integrating blockchain technology patterns within the QR code to verify the certificate. Both of these bibliographic references employ QR codes with the purpose of encoding information in significant documents, such as diplomas and university degrees; however, this method is lacking in terms of confidentiality, which is a necessary tool in counteracting BEC attacks.

Kuacharoen P. et al. [9] propose a method for document verification using QR codes and digital signatures. The process involves composing a message, generating a hash value, and encrypting it with the sender's private key to create a digital signature. The message and signature are combined, compressed, and stored in a QR code on paper for transmission. Upon receiving the document, the receiver scans the QR code to verify the authenticity. This involves checking the integrity of the information, uncompressing and comparing the hash values, and utilizing Optical Character Recognition (OCR) to further validate the printed message. If all checks pass, the message is confirmed as authentic.

This method provides a secure and efficient means of document verification, combining cryptographic techniques with OCR technology to ensure the integrity and authenticity of printed documents. The process outlined above is intended for document authentication and heavily depends on OCR technology, which is associated with numerous drawbacks, such as formatting issues, constraints related to language and character sets, potential misinterpretations of acronyms and abbreviations, among other limitations. Furthermore, the abovementioned solution is based on a trusted third party, which, in some cases when dealing with BEC attacks, is rendered as a drawback. These factors collectively render it an unreliable solution for ensuring security in online communication.

Tkachenko, I. et al. [10], in their research, introduce a novel QR code variant with dual storage levels, designed specifically for document authentication. This innovative QR code, which the authors named the "two-level QR code", incorporates both the public and private storage levels. The public level mirrors the standard QR code storage capacity, making it accessible to any conventional QR code reader. In contrast, the private level is created by substituting the black modules with distinct textured patterns and encoding information using q-ary codes with error correction capabilities. This not only enhances the QR code's storage capacity but also enables the differentiation between the original document and any copies, owing to the sensitivity of these patterns to the print-and-scan (P&S) process. The pattern recognition technique employed to decode the second-level information is versatile, applicable to both private-message-sharing and authentication scenarios. The authentication of the private message is accomplished with ECC-based signatures [11][12]. It relies on the mathematical properties of elliptic curves to provide encryption and decryption capabilities. In ECC, a pair of keys, a public key and a private key, are generated. The public key is used to encrypt the message, while the private key is used to decode (decrypt) it. ECC comes with certain drawbacks, especially when it comes to online communication, such as emails. More specifically, ECC can add complexity to the email security process considered and may not be supported by all email clients and services. Additionally, the abovementioned solution is designed for hard-copy documents, and in order for it to be implemented in online communication systems, factors like replay attacks must be considered thoroughly, especially when it comes to BEC attacks.

3. QR Codes for Digital Authentication

The literature referenced below discusses innovative approaches to authentication. Most of the references utilize QR codes on trusted devices such as mobile phones or through the involvement of a trusted third party. As groundbreaking as these methods may be, their main drawback is the reliance on trusted devices and third-party involvement.

Lu J. et al. [13] propose a methodology for mobile payment authentication that combines visual cryptography (VCS) and aesthetic QR codes. This approach offers three different levels of concealment. The process involves splitting an original QR code into two shadow versions using VCS rules. These two shadow versions are then separately incorporated into the same background image. The results of this embedding process are combined with an identical carrier QR code using a combination of the Reed–Solomon (RS) XOR mechanism and QR code error correction mechanisms. Finally, the two aesthetically enhanced QR codes can be accurately layered to reveal the original QR code as per the defined visual cryptography scheme. While the described solution focuses on enhancing the security in QR code-based mobile payment authentication by splitting the QR code into shadows and embedding it in a carrier QR code, it does not specifically address the issue of business email compromise (BEC) schemes. Specifically, the above proposed solution does not take into consideration advanced encryption techniques, nor does it address the issue of replay attacks.

Liao K.C. [14] propose a QR code-based, one-time-password authentication protocol, which the author claims eliminates the usage of the password verification table in an improved, cost-effective way. While it shows promise, this project focuses on substituting traditional password authentication methods with QR codes through users' mobile devices and is unrelated to safeguarding against BEC schemes.

Oh D. S. et al. [15], in order to address the issue of significant network traffic due to frequent user authentication processes in the existing mobile cloud authentication methods, propose an authentication system that optimizes the network traffic usage in mobile cloud environments by implementing QR codes. However, as the authors claim, this method does not analyze the security vulnerabilities of the suggested system in comparison to existing technologies. Furthermore, the proposed solution in this project concentrates on authenticating users in the Public Cloud, also known as a trusted third party, with the aim of aiding small- and medium-sized businesses, but it does not have any relevance to enhancing online communications, particularly in the context of BEC attacks.

Choi K. et al. [16] propose an anti-phishing, single-sign-on (SSO) authentication model using QR codes. In this proposed architecture, an extended authentication server concentrates the user identifier, server information, and random nonce (random key generated by the server) data and encrypts them with a shared secret key. The secret key is shared by a mobile device with extended authentication. In the next step, the extended-authentication server generates a QR code with the abovementioned encrypted data and also a timestamp. Next, the QR code is scanned from a mobile device, which decrypts the data, generates another random nonce (random key generated from the mobile device), again encrypts all the data plus the password, and creates another QR code with the encrypted data. For the verification phase, the mobile device sends the shared data to an authentication server for validation. The user can then compare the user rand displayed on the web server and the user rand displayed on the mobile device in order to confirm the communication. While this highly promising project offers various advantages, it comes with a notable drawback: the use of an extended-authentication server. Although this server's convenience is apparent, it introduces a potential security risk, as attackers could compromise it. The objective of this project is to improve the user identification and data integrity through the implementation of an identity management system centered around an authentication server. However, this approach may face challenges in its adaptability to business email compromise (BEC) attacks. Instead, token-based identification systems and the use

of anonymous credentials might prove more effective. Furthermore, this approach involves the engagement of a trusted third party in the authentication of both the users and data.

Bairwa et al. [17] created an algorithm for message and data transfer using an authentication token containing six-digit random numbers with the SHA-hash parts of the sender's and receiver's MAC addresses. In this research, the authors use symmetric-key cryptography and especially message authentication codes (MACs). In order to register to the above program, the user must fill the registration form with their username, email, MAC address, and fingerprint. Next, the program generates a password using SHA-256 algorithms, which develop the hash corresponding to the MAC address and the fingerprint. All these data are stored in the user data table. All the above are essential in order for a session key to be created. The session key is developed using random numbers, the SHA hash of the sender MAC address, and the SHA hash of the destination MAC address. While this is very promising work, the algorithm is designed especially for Mobile Ad Hoc Networks (MANETs) [18]. MANETs offer flexibility and autonomy but come with several disadvantages. One notable drawback is that, due to the dynamic nature of MANETs, maintaining secure and efficient routing becomes challenging, leading to potential routing loops and packet drops. Furthermore, another significant disadvantage is the limited network scalability, as the performance degrades as the number of nodes increases. In general, while showing promise, the methodology mentioned above is complicated and inadequate for use as a viable solution to defend against BEC schemes.

Chen C. [19] proposes a QR code authentication method that includes hidden authentication elements like message authentication codes and cryptographic signatures. The entity generating the QR code can create a concealed QR code using the author's enrollment process, where these authentication elements are discreetly incorporated into the code. The key advantage of this proposed method is that the QR code's content remains accessible to standard barcode scanners, and its authenticity can be confirmed offline by authorized users when necessary. In this study, data authentication is achieved through two distinct methods: one involves message authentication codes (MACs), and the other employs digital signatures with asymmetric cryptography. Although the research introduces a novel perspective without the use of trusted devices or external servers, the proposed solution fails to account for certain vulnerabilities, such as replay attacks. Additionally, the BEC Defender utilizes three distinct methods for authentication. These methods consist of a MAC code, authentication of the encrypted sender's MAC address as a unique identifier, and the time differential between the two timestamps, ensuring a three-hour timeframe. Each of these authentication processes plays a unique and vital role in countering BEC attacks.

4. Literature Related to Defense against BEC Attacks

4.1. Technical Methods

There are several ways reported in the literature for defending against BEC attacks that include both technical and non-technical methods. As mentioned in the previous work related to BEC schemes and how to countermeasure them [20], the optimum solution is a combination of technical and non-technical measurements, like those mentioned below:

(1) **DMARC**: The DMARC (Domain-Based Message Authentication, Reporting, and Conformance) email authentication protocol enhances security and prevents email spoofing and phishing attacks. DMARC works in correlation with the SPF (Sender Policy Framework) and DKIM (DomainKeys Identified Mail). The SPF is an email authentication method that allows the domain owner to specify which email servers are authorized to send emails on behalf of their domain. It creates a list of authorized sending IP addresses in the domain's DNS records. When an email is received, the recipient's email server can check the SPF record to verify whether the sending server is authorized to send emails for that domain. DKIM is another email authentication method that adds a digital signature to outgoing emails. The domain owner generates a unique private key and publishes the corresponding public key in the DNS records. The private key is used to generate a digital signature that is attached to the email header. When the recipient's email server receives the email, it can retrieve the public key from the DNS records and use it to verify the digital signature. This ensures the sender's domain authenticity. DMARC builds upon the SPF and DKIM to provide a more comprehensive email authentication framework. It enables the domain owner to define a policy for how the receiving email server should handle emails that fail the SPF or DKIM checks. The DMARC policy can instruct the recipient's server to either quarantine or reject emails that fail authentication. Additionally, DMARC offers reporting mechanisms that grant domain owners the ability to monitor the usage of their domains for email authentication purposes. It generates comprehensive reports containing details about the emails sent on behalf of the domain, including the outcomes of the SPF and DKIM authentication (whether they passed or failed). These reports play a crucial role in assisting domain owners in detecting any unauthorized utilization of their domains, resolving authentication problems, and obtaining valuable insights into potential phishing attempts [21][22]. In conclusion, DMARC offers protection against domain-spoofing emails, preventing them from reaching users' inboxes. Through DMARC, it is possible to block, quarantine, and monitor any malicious emails sent from the controlled domain. Numerous email providers, including Google's Gmail-hosted mailboxes and Microsoft's Office365, offer support for DMARC policies [23]. Typically, mail-filtering techniques like DMARC are specifically crafted to operate based on the header information within emails. The email-filtering policy is formulated to examine both incoming and outgoing emails, aiming to prevent any suspicious messages originating from deceptive domains. However, this approach exhibits vulnerabilities when it comes to impersonation attacks, wherein emails may originate from domains that fall outside the scope of the filter. Furthermore, the limitation of mail-filtering techniques lies in their exclusive focus on the email header. Consequently, they prove ineffective at safeguarding the email system against certain types of attacks, particularly those rooted in content manipulation. For instance, schemes involving fraudulent invoices, in which the email content itself is manipulated, pose a significant challenge, as the current mail-filtering approach does not extend its protective measures to this aspect of the email composition [24]. As Särökaari [25] also mentions in his thesis, deploying the SPF and DMARC is not enough to prevent sophisticated and targeted phishing attacks. Furthermore, if an attacker is able to gain access to an employee's email account, having these countermeasures will not provide any protection, as the attacker is in a position to impersonate the compromised user by having access to their email inbox. Moreover, as Särökaari states, the adoption of these technical security control measures has been largely voluntary, with little penalty for noncompliance;

(2) **Antivirus–antimalware software**: BEC attacks rely on careful and sophisticated planning, involving OSINT investigations to gather critical information about the target. The purpose is to establish psychological leverage and gain valuable insights that can be utilized in future fraudulent emails. However, apart from such meticulous approaches, attackers can employ more direct and intrusive techniques, such as utilizing viruses or malware to compromise the victim's system and extract sensitive data. Key loggers [26] are an example of such malware, recording the victim's keystrokes and thereby capturing sensitive information, like login credentials, usernames, and passwords. Another example is remote-access tools (RATs) [27], which aim at obtaining unauthorized system access for further exploitation. Moreover, BEC attackers often resort to social engineering tactics, such as sending initial emails containing malicious URLs. These deceptive links mislead the unsuspecting victims into installing the malicious software into their systems or entering fraudulent websites that mimic legitimate platforms, like e-banking sites. Once on these fake websites, victims may unknowingly disclose their confidential information, allowing the attackers to perpetrate identity theft or financial fraud or gain unauthorized access to systems. Given the evolving sophistication of BEC attacks and other forms of cyber threats, antivirus and antimalware software has become an indispensable tool for organizations and individuals to protect themselves from potential harm. These security measures aid in detecting and mitigating various forms of malicious software and deceptive tactics employed by cybercriminals, thereby reducing the risk of falling victim to BEC schemes and similar cybercrimes [28];

(3) **Machine learning algorithms**: Machine learning is a field of study within artificial intelligence that focuses on developing algorithms and models capable of learning from data and making predictions or decisions. When it comes to business email compromise (BEC) attacks, machine learning can be a valuable tool in detecting and preventing such threats. Machine learning can help combat BEC attacks in several ways [29]. Firstly, it can be used to analyze historical email data and identify patterns associated with known BEC attacks. By training machine learning models on such data, they can learn to recognize common characteristics, such as suspicious email addresses, language patterns, or anomalies in email headers. Additionally, machine learning algorithms can be employed to analyze email content and attachments in real time. These algorithms can learn from a variety of features, such as the email's structure, sender's reputation, language used, and contextual information. By leveraging these features, the models can identify suspicious emails that exhibit characteristics commonly associated with BEC attacks, such as unexpected changes in account details or urgent requests for funds. Furthermore, machine learning can assist in identifying compromised accounts or unauthorized access attempts. By monitoring the user behavior and detecting deviations from normal patterns, machine learning models can flag potential unauthorized activities, such as login attempts from unfamiliar locations or unusual timeframes. A. Cidon et al. [30] presented BEC-Guard, a detector employed at Barracuda Networks that uses supervised learning to stop business email compromise threats in real time. BEC-Guard detects attacks by using supervised learning algorithms that are trained on an email database that contains millions of emails. These algorithms analyze the header of the email and search for suspicious phrases and links in the email body. Furthermore, BEC-Guard makes use of the public APIs provided by cloud email providers to automatically acquire knowledge about the past communication patterns of each organization. It also employs these APIs to promptly isolate and quarantine emails in real time. According to the writers, BEC-Guard was evaluated using a

commercial dataset comprising over 4000 attacks, achieving a precision of 98.2% and a false-positive rate of less than one in five million emails. A drawback of this methodology is the need to continuously train the algorithm due to the continuous evolution of BEC schemes.

Furthermore, Cohen et al. [31] present a technique for identifying malicious emails through the utilization of machine learning methodologies. By extracting features from complete emails, including the header, body, and attachments, and employing a Random Forest classifier, the approach asserts an impressive accuracy level of 92.9%, with true-positive and false-positive rates standing at 94.7% and 3%, respectively. The dataset used in the performance evaluation was a collection of 33,142 emails (20,307 benign and 12,835 malicious emails) collected between 2013 and 2016. The malicious emails were labeled as such by at least five different antivirus engines using VirusTotal;

(4) **Encryption**: Encryption serves as an effective measure to prevent data breaches by necessitating a pair of cryptographic keys for both the sender and receiver [32]. For example, in identity-based encryption (IBE), the user's email address functions as the public key, and a centralized entity referred to as the Private Key Generator (PKG) is responsible for generating private keys. Following a preliminary authentication process, the private keys are securely transmitted from the PKG to end users through a secure channel. It is worth noting that identity-based encryption (IBE) schemes are susceptible to the key theft problem, enabling the PKG to decrypt any message [32].

Emails can also be safeguarded through various plugins [33]. Mailvelope [34] employs manual key management, requiring users to distribute and handle keys manually, which impacts the usability, especially for novice users. Plugins such as Jumble Mail and Secure Gmail [35] rely on PGP and encrypt messages using their managed keys, requiring end users to trust the provider. Routi et al. [36] conducted a study on PGP with the Mailvelope plugin. Despite considerable enhancements in Mailvelope security, its usability remains low and proves challenging for common users lacking knowledge of public-key cryptography. Other solutions, like Private Webmail, Virtu, and Xmail, generate and distribute encryption keys on their servers while concealing the key management process. However, these solutions are paid, and the unavailability of source codes raises trust concerns for end users;

(5) **Multi-factor authentication (MFA)**: MFA offers a robust method of authentication, demanding two or more verification factors to grant access to a resource [37][38];

(6) **Trusted Third Parties (TTPs)**: Ensuring the secure distribution of public keys to the correct parties can pose significant challenges. The trust placed in the public-key infrastructure (PKI) is of the utmost importance. A trusted third party is often needed to facilitate the provision of public- and private-key pairs. The entire security of the system relies on this trusted entity. Any compromise, whether from external attacks (like server code modification) or internal vulnerabilities, has the potential to undermine the security of the entire system. Consequently, organizations may harbor doubts regarding the trustworthiness of the third party responsible for issuing keys or credentials. Concerns may arise regarding the security practices of the provider, their adherence to regulatory compliance, and their ability to withstand external pressures that could jeopardize the integrity of

the key management process. Organizations may hesitate to place their trust in a third-party key management center that fails to demonstrate adherence to relevant standards and best practices. Additionally, concerns may arise regarding the location of the key management center and its compliance with data sovereignty requirements. Certain regulations mandate that specific data must remain within defined geographical boundaries, and relying on a third-party provider may raise questions about data jurisdiction. The utilization of PKI methods usually requires that organizations entrust an external entity for building secure communication between users, thereby relinquishing a certain degree of control over the cryptographic keys. Some organizations may be reluctant to surrender this control, particularly when dealing with highly sensitive information. Depending solely on a specific key management provider may result in vendor lock-in, making it difficult and costly to switch to an alternative provider. Organizations may have reservations about relying solely on a single provider for a crucial security function. Additionally, the costs associated with utilizing a key management center can be a determining factor, and organizations require assurance that they can conduct audits and verify the key management processes to ensure compliance and security. The lack of transparency from the key management center can pose a significant obstacle in establishing trust. This involvement of TTPs underscores their significance in fostering secure, fair, and trustworthy email interactions, making them valuable components in the architecture of communication systems. According to Kupcu [39], due to the fact that numerous systems depend on trusted third parties (TTPs) for assurances in fairness, security, and efficiency, there is a critical necessity to decentralize the trust placed in these central entities. Moreover, Paulin et al. [40] state that current service providers offer limited solutions dependent on a trusted third party, hindering their applicability across borders, especially in transnational unions such as the EU. The authors introduce a functional certified email system that achieves the fair non-repudiation of receipt without relying on a trusted third party. The proposed protocol involves encrypting a message and splitting it into a chain of parts, with the recipient gradually acquiring each part and generating proofs-of-receipt for the individual segments. This protocol cryptographically prevents the addressee from obtaining the message in case they terminate the protocol prematurely. The universality of the presented system makes it feasible for unobtrusive operation using existing user agents and email providers. Sabir et al. [33] mention that, in contrast to other applications, like social media, email accounts inherently contain more sensitive data, making a hacked email account a potential source of personal information leakage and unauthorized access to various online services. Moreover, despite users relying on service providers for email privacy, this trust is often exploited for targeted advertisements. Additionally, the risk of attackers targeting and compromising numerous email accounts underscores the vulnerability of email systems, especially when considering the danger of an attack on the internal server itself. For the abovementioned reasons, the authors devised a solution using a PKI (public-key infrastructure) similar to that of Proton Mail [41] with the following objectives. Firstly, the system aims to ensure complete end-to-end privacy. Secondly, it strives for significant usability aligned with the Saltzer acceptability principle, aiming to enable users without technical expertise to navigate the system effortlessly, including aspects such as obtaining, distributing, and utilizing cryptographic keys. Thirdly, portability is emphasized, allowing users to switch between public computers without reliance on a specific device. Fourthly, users are not required to install additional hardware or software configurations to use the system. Lastly, the trustworthiness of the application code is highlighted, emphasizing a transparent, cryptographic key-sharing mechanism to instill user confidence.

An interesting work is that of AlSabah et al. [42], which presents a secure end-to-end email communication approach. By employing their innovative certificate-less (CL) key agreement protocol, the method enables users to update their public keys without requiring interaction with the certificate authority (CA).

Moreover, Brown et al. [43] introduced a proxy-based architecture. Proxy-based methods utilize their servers for encrypting and decrypting messages, making them not genuinely end-to-end secure. Jammalamadaka et al. [44] proposed a proxy-based design that necessitates additional hardware (a mobile phone) to execute secure email operations. Another Windows-based system, Opaque-Mail, communicates with mail clients and requires local installation on all users' devices. Additionally, proxy re-encryption, by design, has an insignificant impact on email privacy. Moreover, user trust could be manipulated by introducing backdoors through application source codes.

Finally, Secure/Multipurpose Internet Mail Extensions (S/MIMEs) serve as an encryption standard akin to PGP, ensuring the security of email content. Built on public-key cryptography, S/MIMEs mandate the involvement of certificate authorities (CAs) in issuing certificates for both the sender and receiver. This approach necessitates mutual trust in the CA. Despite some companies opting for self-issued certificates, these are often perceived as untrustworthy, potentially introducing security vulnerabilities. Additionally, S/MIMEs fall short in safeguarding users against Vendor Email Compromise (VEC) attacks, particularly when utilizing servers that store users' private keys on the servers. It is crucial to acknowledge that no single method can offer comprehensive protection against fraudulent schemes. While S/MIMEs provide the confidentiality and integrity of contents, they are considered weak against VEC attacks. Consequently, it is advisable to employ a combination of security measures, including TLS, S/MIMEs, and the suggested method, to fortify a company's defense against such attacks [24];

(7) **Digital signatures**: Digital signatures in email communication are instrumental in fortifying the security and reliability of electronic exchanges. These signatures, generated through cryptographic algorithms, assure the authenticity of the sender and the integrity of the message content. This form of security prevents unauthorized access and tampering during transmission, offering a vital defense against cyber threats. Moreover, digital signatures provide a crucial element of non-repudiation, making it challenging for senders to deny their involvement in a specific message. This not only enhances accountability but also minimizes the risk of disputes over message origins. In an environment where sensitive information is regularly shared, the adoption of digital signatures instills confidence, establishing a secure foundation for electronic communication [45][46]. Digital signatures, while offering significant advantages, are not without their drawbacks. A notable vulnerability is the issue of "unobservability" in electronic documents. This means that, in certain cases, the content of a digitally signed document may be concealed or difficult to discern. According to Lax et al. [47], unlike traditional documents that can be interpreted by humans through direct observation, digital documents rely on machine-level interpretation and require complex instruments such as computers for viewing and signing. This inherent complexity introduces vulnerabilities, particularly in ensuring the consistency and reliability of these instruments. The unobservability of digital documents poses a challenge to the direct link between the signature and the information's integrity, making it inherently weaker compared to handwritten signatures. Despite technical measures addressing bit-level modifications, concerns persist regarding the reliability of the instruments used

for viewing and signing documents, rendering digital signatures inherently weak. The paper highlights various vulnerabilities resulting from this unobservability and explores potential solutions, emphasizing the balance between security and usability in the context of digital signatures. Malicious actors can exploit disadvantages like the abovementioned to their advantage, compromising the transparency and verifiability that digital signatures aim to provide. To address this, there is a critical need for secure and efficient verification methods. Advanced algorithms can play a pivotal role in enhancing the verification process, ensuring that the integrity and authenticity of digitally signed documents are upheld [48]. Implementing sophisticated algorithms can mitigate the risks associated with unobservability, making it more challenging for malicious actors to manipulate or conceal electronic content.

4.2. Non-Technical Methods

- **Employee training**: Ongoing employee training is vital to empower staff in identifying, reporting, and handling BEC attacks effectively. It is especially crucial to provide regular training to sensitive sectors, like the financial department, focusing on social engineering techniques and BEC schemes. Employees should also exercise caution when dealing with hyperlinks, attachments, name misspellings, sudden wire transfer requests, or altered account details. Encouraging the verification of vendor information is equally essential and strongly recommended. It is important to recognize that social engineering and BEC schemes are continuously evolving, underscoring the necessity for continuous and up-to-date training sessions. By remaining vigilant and well informed, employees can play a crucial role in safeguarding the organization against threats like BEC attacks [49][50];

- **Social engineering departments**: Creating a dedicated social engineering department is essential when it comes to large companies. This department should consist of employees who have undergone specialized training in social engineering and open-source intelligence (OSINT) investigations. Leveraging OSINT tools, they can conduct thorough investigations of high-profile targets within the company to identify potential data breaches and leaks. Utilizing free online services like Have I Been Pwned [51] and DeHashed [52], they can assess vulnerabilities and gather crucial information to safeguard against BEC attempts. Recognizing that the information gathered could be exploited by malicious attackers in order to make the profile of a target, understanding the existing gaps and potential compromises in the company's profile becomes crucial. By proactively identifying and addressing these weaknesses, the organization can effectively prevent and detect future BEC attacks, fortifying its cybersecurity defenses [53];

- **Defining policies**: To bolster security measures, the implementation of a set of comprehensive policies and internal guidelines that prioritize safeguarding information sharing and financial transactions is needed. By defining and adhering to these policies, the organization can significantly mitigate the risks associated with BEC attacks and enhance their overall cybersecurity. Characteristic examples of these policies are as follows:

    - Prohibition of the use of email requests for fund transfers and, instead, mandating the presence of multiple individuals or at least a vocal confirmation for financial transactions;

- Strong communication protocols for phone-based interactions by enforcing identity verification questions to prevent unauthorized data disclosure;
- Encouragement of the swift reporting of any security incidents to enable quicker action and resolution;
- Endorsement of strong password policies.

When it comes to safeguarding against business email compromise (BEC) attacks, there are a variety of protective measures, each with its own set of advantages and drawbacks, as discussed earlier.

DMARC, for instance, is a potent tool that serves to shield against domain spoofing, ensuring the integrity and authenticity of emails through the use of digital signatures in outgoing messages. However, determined attackers armed with lookalike domains or adept social engineering techniques can bypass this defense mechanism by manipulating email addresses, aiming to deceive recipients.

Antivirus and antimalware software plays a crucial role in guarding users against malicious URLs and programs that exploit system vulnerabilities. Nevertheless, its effectiveness relies heavily on widespread adoption and regular updates, and it remains susceptible to emerging threats like zero-day exploits. Furthermore, it is ill equipped in countering social engineering techniques.

Machine learning algorithms offer promise in classifying emails and raising the awareness of potential red flags by scrutinizing data and identifying patterns associated with BEC attacks. However, to function efficiently, machine learning requires the analysis of large amounts of data, particularly within email body text.

Encryption, as previously noted, provides substantial security benefits. Still, it is not without its share of challenges and disadvantages, including complexity in its implementation, the need for diligent key management, compatibility issues across various platforms, and the added processing overhead it demands.

Multi-factor authentication (MFA), a widely endorsed security practice, furnishes an additional layer of protection for user accounts. Nonetheless, it introduces its own set of challenges. Users may find MFA less convenient, particularly during the setup phase. Compatibility issues may arise, especially when dealing with diverse systems and applications. Moreover, MFA does not eliminate the risk of phishing attacks, especially if users are not adequately educated about its usage and potential vulnerabilities. Additionally, when it comes to BEC attacks, recipients have no way of discerning whether the sender employed MFA, leaving room for uncertainty.

Finally, non-technical strategies for guarding against BEC attacks, such as employee training initiatives, policy formulation, and the establishment of specialized departments, like those focusing on social engineering, offer valuable layers of defense. However, they are contingent on continuous education and policy updates, making them susceptible to the ever-evolving nature of BEC attacks. These approaches also rely heavily on human factors, which introduce their own unique challenges. In essence, while these non-technical strategies are valuable components of a comprehensive BEC defense strategy, they require constant vigilance and adaptation. Cybercriminals continually refine their tactics, which necessitates ongoing education and policy refinement.

Moreover, they demand a deep understanding of the human element in security, acknowledging that the human factor can both bolster and undermine the effectiveness of these defenses.

References

1. Oberlo. Available online: https://www.oberlo.com/statistics/how-many-emails-are-sent-per-day (accessed on 1 November 2023).
2. Pastor-Galindo, J.; Nespoli, P.; Mármol, F.G.; Pérez, G.M. The not yet exploited goldmine of OSINT: Opportunities, open challenges and future trends. IEEE Access 2020, 8, 10282–10304.
3. Al-Musib, N.S.; Al-Serhani, F.M.; Humayun, M.; Jhanjhi, N.Z. Business email compromise (BEC) attacks. Mater. Today Proc. 2021, 81, 497–503.
4. Cross, C.; Gillett, R. Exploiting trust for financial gain: An overview of business email compromise (BEC) fraud. J. Financ. Crime 2020, 27, 871–884.
5. FBI. Internet Crime Report. 2022. Available online: https://www.ic3.gov/Media/PDF/AnnualReport/2022IC3Report.pdf (accessed on 25 April 2023).
6. González-Granadillo, G.; González-Zarzosa, S.; Diaz, R. Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. Sensors 2021, 21, 4759.
7. Singhal, A.; Pavithr, R.S. Degree certificate authentication using QR code and smartphone. Int. J. Comput. Appl. 2015, 120, 38–43.
8. Aini, Q.; Rahardja, U.; Tangkaw, M.R.; Santoso, N.P.L.; Khoirunisa, A. Embedding a blockchain technology pattern into the QR code for an authentication certificate. J. Online Inform. 2020, 5, 239–244.
9. Kuacharoen, P.; Warasart, M. Paper-based document authentication using digital signature and qr code. In Proceedings of the International Conference on Computer Engineering and Technology, Bangkok, Thailand, 12–13 May 2012; Volume 40, pp. 1–5.
10. Tkachenko, I.; Puech, W.; Destruel, C.; Strauss, O.; Gaudin, J.M.; Guichard, C. Two-level QR code for private message sharing and document authentication. IEEE Trans. Inf. Forensics Secur. 2015, 11, 571–583.
11. Kapoor, V.; Abraham, V.S.; Singh, R. Elliptic curve cryptography. Ubiquity 2008, 9, 1–8.
12. Kazmirchuk, S.; Ilyenko, A.; Ilyenko, S. Digital Signature Authentication Scheme with Message Recovery Based on the Use of Elliptic Curves. In Advances in Computer Science for Engineering and Education II; Hu, Z., Petoukhov, S., Dychka, I., He, M., Eds.; Springer: Berlin/Heidelberg, Germany, 2020; pp. 279–288.

13. Lu, J.; Yang, Z.; Li, L.; Yuan, W.; Li, L.; Chang, C.C. Multiple schemes for mobile payment authentication using QR code and visual cryptography. Mob. Inf. Syst. 2017, 2017, 4356038.
14. Liao, K.C.; Lee, W.H. A novel user authentication scheme based on QR-code. J. Netw. 2010, 5, 937–941.
15. Oh, D.S.; Kim, B.H.; Lee, J.K. A Study on Authentication System Using QR Code for Mobile Cloud Computing Environment. In Future Information Technology. Communications in Computer and Information Science; Park, J.J., Yang, L.T., Lee, C., Eds.; Springer: Berlin/Heidelberg, Germany, 2011; Volume 184.
16. Choi, K.; Lee, C.; Jeon, W.; Lee, K.; Won, D. A mobile based anti-phishing authentication scheme using QR code. In Proceedings of the International Conference on Mobile IT Convergence IEEE, Gumi, Republic of Korea, 26–28 September 2011; pp. 109–113.
17. Bairwa, A.K.; Joshi, S. Mutual authentication of nodes using session token with fingerprint and MAC address validation. Egypt. Inform. J. 2021, 22, 479–491.
18. Kumar, M.; Mishra, R. An overview of MANET: History, challenges and applications. Indian J. Comput. Sci. Eng. 2012, 3, 121–125.
19. Chen, C. QR Code Authentication with Embedded Message Authentication Code. Mob. Netw. Appl. 2017, 22, 383–394.
20. Papathanasiou, A.; Liontos, G.; Liagkou, V.; Glavas, E. Business Email Compromise (BEC) Attacks: Threats, Vulnerabilities and Countermeasures-A Perspective on the Greek Landscape. J. Cybersecur. Priv. 2023, 3, 610–637.
21. Kucherawy, M.; Elizabeth, Z.; Domain-Based Message Authentication, Reporting, and Conformance (DMARC). RFC. 2015. Available online: https://www.rfc-editor.org/rfc/rfc7489 (accessed on 10 November 2023).
22. Nightingale, J.S. Email Authentication Mechanisms: DMARC, SPF and DKIM; US Department of Commerce, National Institute of Standards and Technology: Gaithersburg, MD, USA, 2017.
23. Derouet, E. Fighting phishing and securing data with email authentication. Comput. Fraud Secur. 2016, 2016, 5–8.
24. Teerakanok, S.; Yasuki, H.; Uehara, T. A Practical Solution against Business Email Compromise (BEC) Attack using Invoice Checksum. In Proceedings of the 2020 IEEE 20th International Conference on Software Quality, Reliability and Security Companion (QRS-C), Macau, China, 11–14 December 2020; pp. 160–167.
25. Särökaari, N. Phishing Attacks and Mitigation Tactics. Master’s Thesis, University of Jyväskylä, Jyväskylä, Finland, 2020. Available online:

https://jyx.jyu.fi/bitstream/handle/123456789/72569/1/URN%3ANBN%3Afi%3Ajyu-202011116604.pdf (accessed on 19 November 2023).

26. Sagiroglu, S.; Canbek, G. Keyloggers: Increasing threats to computer security and privacy. IEEE Technol. Soc. Mag. 2009, 28, 10–17.
27. Boyd, I.M. The Fundamentals of Computer Hacking; SANS Institute: Rockville, MD, USA, 2021.
28. Nisha, T.N.; Bakari, D.; Shukla, C. Business E-mail Compromise—Techniques and Countermeasures. In Proceedings of the International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE) IEEE, Noida, India, 4–5 March 2021; pp. 217–222.
29. Atlam, H.F.; Oluwatimilehin, O. Business Email Compromise Phishing Detection Based on Machine Learning: A Systematic Literature Review. Electronics 2023, 12, 42.
30. Cidon, A.; Gavish, L.; Bleier, I.; Korshun, N.; Schweighauser, M.; Tsitkin, A. High Precision Detection of Business Email Compromise. In Proceedings of the 28th USENIX Security Symposium (USENIX Security 19), Santa Clara, CA, USA, 14–16 August 2019; pp. 1291–1307.
31. Cohen, A.; Nissim, N.; Elovici, Y. Novel Set of General Descriptive Features For Enhanced Detection of Malicious Emails Using Machine Learning Methods. Expert Syst. Appl. 2018, 110, 143–169.
32. Shamir, A.; Identity-Based Cryptosystems and Signature Schemes. In Ibn Al-Haitham Journal for Pure and Applied Sciences (IHJPAS) Special Issue; 2021; Volume 2021, pp. 82–95. Available online: https://api.semanticscholar.org/CorpusID:1402295 (accessed on 27 November 2023).
33. Sabir, M.; Yousaf, M. Design and Implementation of an End-to-End Web based Trusted Email System. Procedia Comput. Sci. 2018, 141, 231–238.
34. Mailvelope Inc. Available online: https://www.mailvelope.com/en (accessed on 27 November 2023).
35. Secure Gmail Plugin. Available online: https://www.securegroup.com/encryption/ (accessed on 29 November 2023).
36. Ruoti, S.; Andersen, J.; Zappala, D.; Seamons, K. Why Johnny still, still can’t encrypt: Evaluating the usability of a modern PGP client. arXiv. 2015, arXiv:1510.08555. Available online: https://api.semanticscholar.org/CorpusID:5189682 (accessed on 29 October 2023).
37. Ometov, A.; Bezzateev, S.; Mäkitalo, N.; Andreev, S.; Mikkonen, T.; Koucheryavy, Y. Multi-Factor Authentication: A Survey. Cryptography 2018, 2, 1.
38. Papathanasaki, M.; Maglaras, L.; Ayres, N. Modern Authentication Methods: A Comprehensive Survey. In AI, Computer Science and Robotics Technology; IntechOpen: London, UK, 2022.

39. Küpçü, A. Distributing trusted third parties. SIGACT News 2013, 44, 92–112.
40. Paulin, A.; Welzer, T. A universal system for fair non-repudiable certified e-mail without a trusted third party. Comput. Secur. 2013, 32, 207–218.
41. ProtonMail, Proton Technologies AG Plugin. Available online: https://protonmail.com/ (accessed on 28 November 2023).
42. AlSabah, M.; Tomescu, A.; Lebedev, I.; Serpanos, D.; Devadas, S. PriviPK: Certificate-less and secure email communication. Comput. Secur. 2017, 70, 1–15.
43. Brown, I.; Snow, C. A proxy approach to e-mail security. Softw.-Pract. Exp. 1999, 29, 1049–1060.
44. Jammalamadaka, R.; Horst, T.; Mehrotra, S.; Seamons, K.; Venkatasubramanian, N. Delegate: A Proxy Based Architecture for Secure Website Access from an Untrusted Machine. In Proceedings of the 22nd Annual Computer Security Applications Conference (ACSAC), Miami Beach, FL, USA, 11–15 December 2006.
45. Nurhaida, I.; Ramayanti, D.; Riesaputra, R. Digital signature & encryption implementation for increasing authentication, integrity, security and data non-repudiation. Int. Res. J. Comput. Sci. 2017, 4, 4–14.
46. Rai, A.K.; Singh, M.; Sudheendramouli, H.C.; Panwar, V.; Balaji, N.A.; Kukreti, R. Digital Signature for Content Authentication. In Proceedings of the International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI), Chennai, India, 25–26 May 2023; pp. 1–6.
47. Lax, G.; Buccafurri, F.; Caminiti, G. Digital Document Signing: Vulnerabilities and Solutions. Inf. Secur. J. A Glob. Perspect. 2015, 24, 1–14.
48. Kasodhan, R.; Gupta, N. A New Approach of Digital Signature Verification based on BioGamal Algorithm. In Proceedings of the 3rd International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 27–29 March 2019; pp. 10–15.
49. Jensen, M.L.; Dinger, M.; Wright, R.T.; Thatcher, J.B. Training to mitigate phishing attacks using mindfulness techniques. J. Manag. Inf. Syst. 2017, 34, 597–626.
50. Burgess, A.; Jackson, T.; Edwards, J. Email training significantly reduces email defects. Int. J. Inf. Manag. 2005, 25, 71–83.
51. HaveIBeenPwned (HIBP). Available online: https://haveibeenpwned.com (accessed on 2 November 2023).
52. DeHashed. Available online: https://www.dehashed.com (accessed on 20 October 2023).
53. Bazzell, M. Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information, 3rd ed.; CreateSpace Independent Publishing Platform: Scotts Valley, CA, USA,

2016; pp. 154–166.