Materials Today: Proceedings xxx (xxxx) xxx

Contents lists available at ScienceDirect

Materials Today: Proceedings

journal homepage: www.elsevier.com/locate/matpr

Business email compromise (BEC) attacks

Norah Saud Al-Musib [a], Faeiz Mohammad Al-Serhani [a], Mamoona Humayun [a,*], N.Z. Jhanjhi [b]

[a] College of Computer and Information Sciences, Jouf University, Al-Jouf, Saudi Arabia
[b] School of Computer Science and Engineering (SCE), Taylor's University, Malaysia

ARTICLE INFO

Article history:
Available online xxxx

Keywords:
Business email compromise (BEC)
Email phishing
Email threats
Cybercrime

ABSTRACT

Cybercrime is a daily threat against organizations and partners of all sizes and with the rapid development of technology and the great dependence on it in some transactions, a type of serious threats has emerged that pose a high degree of risk to companies and organizations that rely on financial transactions in their work. This type of threat is called Business Email Compromise (BEC), which is a type of email phishing for financial purposes. This attack increased dramatically and caused very high financial losses to companies, especially in the period of remote work and in the Corona crisis, as it increased in the third quarter of the century of this year by 94%. This type of threat does not require a high percentage of knowledge, experience, or skills in deception and fraud, it requires only a reasonable level of social engineering. In this paper, we contribute to analyze this threat is, how it occurs, ways to avoid it or reduce its incidence, and impact on the organization.

Selection and peer-review under responsibility of the scientific committee of the International Virtual Conference on Sustainable Materials (IVCSM-2k20).

1. Introduction

The advancement of technologies and the growth in the usage of public Internet-based resources such as cloud computing, social networks, as well as online money processing resources have dramatically raised organizations' cyberattack threats. Cybercriminals exploit email networks to carry out cyberattacks on companies for financial benefits, as emails have become a common mode of communication worldwide [127].Fig. 1.Fig. 2..Fig. 3.

The newest tool in the internet-criminals is spear phishing in the type of executive spoofing threats [222], One of the most important is what is known as BEC scams, "CEO fraud" and "man-in-the-middle scams[3].BEC attacks are complex email scams that threaten organizations as part of their standard procedures that perform wire transfers. In BEC assaults, social engineering is a central component in which cybercriminals have been very effective in defrauding corporations and workers worldwide [12930]. In 2018, 20,373 BEC / EAC reports were issued by the FBI's Internet Crime Complaint Center with average damages including over $1.2 billion [218].

Traditional protection strategies have not been effective in stopping BEC threats, such as spam filters, since they are customary and appear genuine and have not been observable by technological security solutions [1]. A URL or an attachment is used in just 3% of BEC assaults. With conventional filtering technologies, the lack of a malicious payload in BEC attacks renders them difficult to detect [5]. It is increasingly used because it is successful and hard to examine and prosecute [2]. This planner exists globally and no silver bullets to deter such attacks [2]. It is that, unlike stuff such as attacks using banking trojans or other forms of criminal ransomware, which could require a greater degree of skill, it does not require an especially high level of technical skill to execute, other than having a first name and the last name and the name of whomever they want to address, they don't do much analysis[6].

The contribution to this paper is to provide detailed awareness about BEC attacks due to its rapid development during this time due to the heavy reliance on the internet and remote work strategy, especially in the time of Covid-19, as it causes a lot of damage and financial losses to organizations and individuals. As it increased in the third quarter of this year to 94% compared to the second and first quarter, it was the second more than the first by 112% in the number of attacks in invoice and payment fraud BEC, It is expected to increase in the future if training is not completed and precautions are taken to reduce this threat [151617].

* Corresponding author.
E-mail addresses: fmserhani@ju.edu.sa (F. Mohammad Al-Serhani), mahumayun@ju.edu.sa (M. Humayun), noorzaman.jhanjhi@taylors.edu.my (N.Z. Jhanjhi).

https://doi.org/10.1016/j.matpr.2021.03.647
2214-7853/© 2021 Elsevier Ltd. All rights reserved.
Selection and peer-review under responsibility of the scientific committee of the International Virtual Conference on Sustainable Materials (IVCSM-2k20).

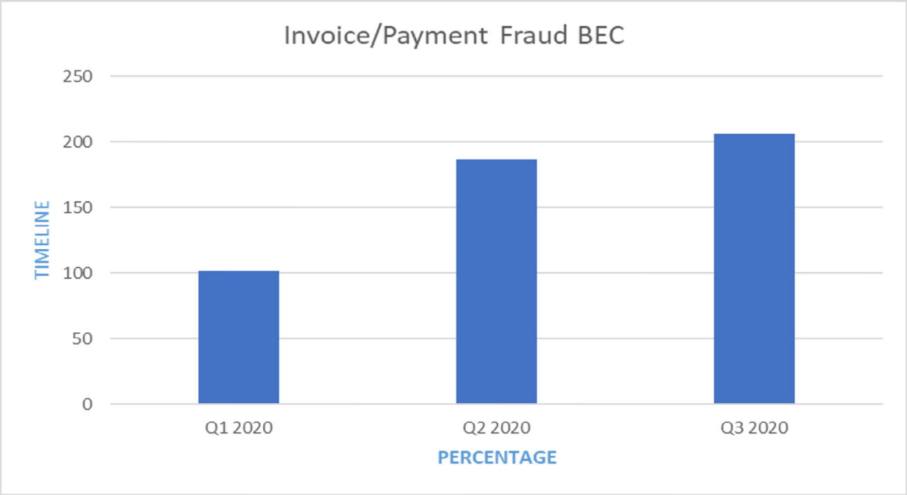
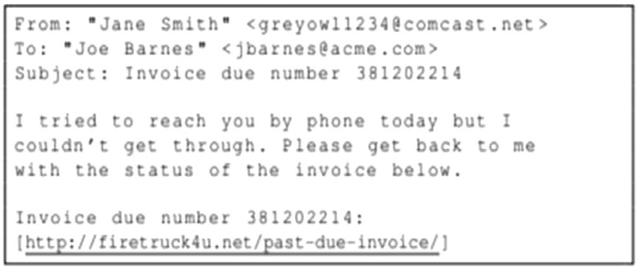


Fig. 1. BEC increased during the first three quarters of 2020.

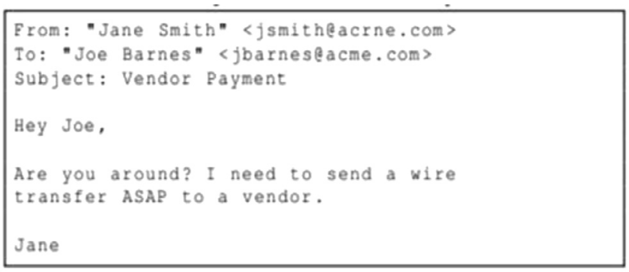


```
From: "Jane Smith" <greyowl1234@comcast.net>
To: "Joe Barnes" <jbarnes@acme.com>
Subject: Invoice due number 381202214

I tried to reach you by phone today but I
couldn't get through. Please get back to me
with the status of the invoice below.

Invoice due number 381202214:
[http://firetruck4u.net/past-due-invoice/]
```

Fig. 2. Fake bill fraud [13].



```
From: "Jane Smith" <jsmith@acrne.com>
To: "Joe Barnes" <jbarnes@acme.com>
Subject: Vendor Payment

Hey Joe,

Are you around? I need to send a wire
transfer ASAP to a vendor.

Jane
```

Fig. 3. CEO account fraud [13].

Also in this paper, we explain some of the methods that can help prevent and detect such an attack from happening dramatically.

This paper is organized as follows: Section 2 will be discussing related work, section 3 describes background on business email compromise (BEC) attacks, Section4 discusses types of BEC attacks, Section 5 shows the working of BEC attack, section 6 provides the ways to help spot BEC attacks, section 7 describes the methods for protection against BEC attacks, section 8 conclude the paper.

2. Related work

In this part, the studies related to woks that are relevant in this field are clarified and the solutions presented are discussed and summarized as indicated in Table 1.

This paper [2], dealt with most of the BEC topics. The purpose of this paper was to explain the fraud schemes known as business email hacking and executive identity impersonation. Whereas, emails can be very accurate and persuasive given that it comes from a source believed to be reliable and there are two most common variations of BEC schemes; the urgent transaction request from the boss and the strong-arm vendor request. Among the methods proposed to protect financial organizations and companies from this risk,this paper proposes multi-factor authentication. it also indicated the importance of verifying the identity of the message owner by voice call to verify that the person is not unknown to them and also trying to discover the EBC risk before it occurs to reduce damage and losses. Also, the focus was on training, it considers training equivalent to validation and verification because if the employees and management did not have the knowledge or culture of BEC risk and ways to prevent it, the benefit from technical methods is greatly reduced.

In paper [7], the focus was on what BEC attack is and how to protect from it in particular as they are clear business email compromise is a kind of internet-based fraudulence that usually aim at employees through methods such as social engineering and device interferences with access to corporate finances. The use of conventional anti-phishing strategies to detect this attack vector, BEC forgery, can be challenging if not impossible. They also noted that the FBI reports that the pandemic of COVID-19 and relevant public health and government closing requests have increased the risk even further. They also clarified that taking the victim's webmail password is among the most significant forms of BEC attack, a swindler who obtained illegal access to a victim's company email account. They also discussed how to avoid being a victory of BEC attacks All parties must have sufficient cybersecurity controls on their email systems for and party to be safe. It is not enough if there are sufficient controls for only one side. Therefore, in the deal, every party should inform the other parties and ensure that those other parties also have suitable controls. insure that the payer agency initiates voice authentication since only an outbound call to a recognized mobile number can be believed; caller ID can be deceiving in some jurisdictions on an inbound call and must not be believed as a means of verifying the caller. Each password chosen for an email account must be special should never be like or similar to any other web account password that was used by the user. They also touched on the FBI's guidelines for defense.

Paper [8] aims to examine existing awareness of business email compromise (BEC) fraud or methods that specifically target organizations for financial benefit, through the manipulation of trusted relationships. BEC fraud affects organizations globally and since 2016 it is reported that netted criminals have more than the US

Table 1
Summary of Literature Review.

The paper	Year of Publication	Suggestion	Solutions
David Zweighaft.[2]	2017	Explain the fraud schemes known as business email hacking and executive identity impersonation.	Multi-factor authentication. Training the staff.
Jennifer C. Archie et al.[7]	2020	What this attack is and how to protect from it in particular in COVID-19.	All parties must have sufficient cybersecurity controls on their email systems for and party to be safe. Ensure that the payer agency initiates voice authentication since only an outbound call to a recognized mobile number can be believed. Each password chosen for an email account must be special should never be like or similar to any other web account password that was used by the user. FBI's guidelines for defense.
Cassandra Cross et al.[8]	2020	Examine existing awareness of business email compromise (BEC) fraud or methods that specifically target organizations for financial benefit, through the manipulation of trusted relationships.	Technological solutions, such as ensuring that computer software is up-to-date, anti-malware and end-point protection systems, and digital email signing, analyzing historical email trends and non-technical solutions, ensuring that computer programs are up-to-date, anti-malware. The non-technical solution, such as a key protection mechanism against BEC fraud.
Seiko Myojin et al. [9]	2020	Focusing on the channel theory to avoid a threat of BEC.	Benefits of channel theory to avoid the threat of BEC.
Shahar Aviv et al. [1]	2019	Define components for evaluating business email compromise identification capability accepted by the cybersecurity expert group.	Use the Delphi method using cybersecurity experts to detect BEC.
Bridget Opazo et al.[14]	2017	Given a mechanism to use in self-defense for the creation of a client-side sentinel.	Help deter effective email spoofs in the ongoing escalation of BEC and the fraud against private individuals. Their solution will be to alert the user whether, based on automatic email source code tests, an email is suspect.
Asaf Cidon et al.[13]	2019	Implemented BEC-Guard, a detection system used in Barracuda Net operations.	Break the issue of classification into two sections, one evaluating the email header and the other applying natural language processing to identify BEC-related phrases or suspicious connections in the email body.

$26 billion. Given the sheer magnitude of these casualties, there is a lack of academic research seeking to better grasp this criminality kind, and prevent it from occurring. Financial advantage is the overall purpose of any dishonest strategy. As the name suggests, BEC fraud targets corporations as victims rather than people. It tries, through a variety of dishonest methods, to acquire money or personal information from corporations. Many BEC methods depend on the perpetrator, such as the CEO or other senior management within an organization, taking on the persona of a genuine individual or corporation. This could be to gain direct access to a device or to acquire the requisite credentials for future access through the use of malware and/or phishing. To trick the recipient, phishing emails are likely to mimic that of a real individual or an organization. If a perpetrator can tailor the specifics of their strategy to the particular flaws or weaknesses of the tailor, fraud is effective. The more the attacker knows about the target business, the more it is probable that a BEC scam would succeed. Legislative protections against the unauthorized disclosure of personal information (such as the General Data Security Regulation) have been strengthened, granting companies more responsibility for protecting any information they have. Companies that do not safeguard user information may be responsible for infringements that have occurred as part of the BEC scam. Other costs associated with BEC fraud victimization that are yet to be recognized are also likely to occur. These include physical health decline, a reduction in mental and psychological well-being, depression, unemployment, dissolution of marriages, homelessness, and, in severe cases, the concept of suicide and suicide. Companies are trying a variety of different approaches to avoid the success and efficacy of BEC fraud through their organizations. This involves a range of technological solutions, such as ensuring that computer software is up-to-date, anti-malware and end-point protection systems, and digital email signing can also secure goals-against BEC fraud, analyzing historical email trends and non-technical solutions, ensuring that computer programs are up-to-date anti-malware and endpoint security systems. And employee consciousness is a non-technical solution, such as a key protection mechanism against BEC fraud. BEC fraud is a continuing problem for all corporations, people, the police, and the community as a whole.

This paper [9] focuses on the channel theory, they studied the email contact scenario based on the BEC event. Their research portrayed a cognitive trap and the decision-making mechanism of the consumer. They lead to provide practical information that helps the user, by forecasting logical traps, to alert him. Clear contact was an example of BEC in this article. But they did explain that their idea had to be reformulated for a longer and more complicated conversation. Their research has struggled to enter the point of assessing if the malice was in the email partner. This article, though, maybe a concern when the recipient reconsiders their correspondence on the premise that the malice can be triggered by the email associate. In the end, it was made clear that they will future research to judge hatred is.

The primary objective ofthe research study [1] was to define components for evaluating business email compromise identification capability accepted by the cybersecurity expert group. Also, this study aimed to create a BEC awareness training module approved by a specialist for business professionals who perform and have the authority to authorize wire transfers. These consumers come under the BEC CEO system where the email address of the CEO or other company official is either compromised or spoofed and leveraged to order a wire transfer to the fake account. The BECD calculation instrument was created through the Delphi method using cybersecurity experts. In constructing a measuring instrument, the Delphi process is an optimal approach to obtaining an expert panel consensus.

Paper [14] proposed that users would be given a mechanism to use in self-defense for the creation of a client-side sentinel that could help deter effective email spoofs in the ongoing escalation of BEC and the fraud against private individuals. Their solution will be to alert the user whether, based on automatic email source code tests, an email is suspect. It is also fairly straightforward to detect an impostor by viewing the email source code. If these emails manage to get through server encryption, even from the user side based on other signs, such as poor grammar, they are also always easy to find. There are other indications, less evident in the case of an expert attack, that an automatic client-side sentinel might search and then warn the user to exercise caution. Sentinel software could search for an SPF soft failure allowed by the server, it could compare separate fields from/reply-to fields for accuracy to defend against novice spoofs, and it could check for unusual look-alike characters in a Reply-To field email address that could suggest a spoof attempt. The sentinel program may be set up in the event of repeated false-positive warnings to allow a white-list of accepted email addresses as well as accepted domains. Once, according to suggested protocols, the recipient had checked the email's authenticity, he could white-list the email. In potential email communications, the program will collect the return-path, from, and reply-to field entries and just compare those fields. This approach will shield the customer from potential spoofs while eliminating multiple warnings that are distracting. To support organizations with accountability mechanisms, the app may also be designed to log warnings. And since the app will be client-facing, it might be possible to create versatility to search the body of an email for text items that the recipient has marked as problematic. Based on the data, additional warnings may be programmed. The principle of sentinel software is easy enough to extend to any computer, so it will no longer be a challenge with the BYOD community.

Paper [13], authors implemented BEC-Guard, a detection system used in Barracuda Net operations that uses a supervised learning algorithm to avoid company email compromise attacks in real-time. Since July 2017, BEC-Guard has been in development and is part of the Barracuda Sentinel email protection product. By depending on stats for historical email habits that can be accessed through cloud email provider APIs, BEC-Guard identifies attacks. When developing BEC-Guard, the two major difficulties are the need to mark millions of emails to prepare the classifiers and to correctly educate the classifiers when it is very unusual for staff impersonation emails to happen, which may skew the classification. Their main insight is to break the issue of classification into two sections, one evaluating the email header and the other applying natural language processing to identify BEC-related phrases or suspicious connections in the email body. BEC-Guard uses cloud email providers' public APIs both to dynamically understand each organization's past contact patterns and to quarantine emails in real-time. On a commercial database consisting of upwards of 4,000 threats, BEC-Guard was tested and revealed an accuracy of 98.2% and a false positive rate of less than one in 5 million emails.

3. Background on business email compromise (BEC) attacks

Business email compromise (BEC) is a type of fraud that persuades victims to wire large sums of funds or send sensitive information to criminally managed accounts through a team of cybercriminals. It is encouraged by the assumption of victims that a trustworthy party is asking them or instructing them to do so [102129]. Eighty-five percent of all BEC attacks are immediate requests intended to get a fast reaction. 59% are requesting assistance, and 26% are talking about supply [5]. A BEC attack is a dynamic cyber assault targeted at companies that routinely perform financial transactions and exploit malicious emails from social engineering to force an employee to perform a wire transfer [1]. On weekdays, 91 percent of BEC assaults take place. Attackers attempt as hard as possible to imitate corporate behavior, often sending an email within the normal operating hours of the compromised account to make them seem more credible and trusting [5]. Often Office 365 (or Google suites) is exposed in several BEC situations when two-factor authentication (2FA) has not been allowed [10]. To mount an attack, hackers also use common, free, web-based email services, including Gmail and Yahoo. The most popular email range used in BEC attacks is Gmail. Attacks can also come from hacked email addresses, making it much harder to identify them [5].The important features of a cyber assault on an employee spoofing [2]

- A senior executive or a central distributor or provider makes email demands.
- With rather slight, subtle variations, the email account is significantly identical to the alleged sender's account.
- In the email, other workers are linked to or copied.
- payouts demanded are owed to outside the country bank.
- When the executive is trying to travel and cannot be reached, inquiries arise.
- Concerning the prepayment, there is an aspect of immediacy or confidentiality.
- The quantity is in the usual payment range in order not to trigger doubt.

4. Types of bec attack

Five forms of business email compromise (BEC) have been reported by the US Federal Bureau of Investigation (FBI),are described as follows[6]:

- Working with a foreign supplier, or what is called a fake bill fraud, where the attacker exploits an existing relationship between two companies and asks to pay an invoice where the employee believes it is actually from one of the suppliers to the customer, but the message contains the attacker's bank account as shown in Image 1 [13].
- Personal fraud or CEO account, and this often occurs in this type of attack, where the attacker quickly requests a bank transfer from the employee in charge of bank transfers, as the attacker deludes the employee that this request is from a senior official because he asks that the bank transfer process be done as soon as possible. Possible and without a phone call because it is busy as shown in Image 2 [13 20].
- An email hack of a payments employee and the attacker makes payments to his account or financial payment requests.
- personality fraudulent of an executive director or lawyer, where the attacker requests bank transfers from the target company, and it is often done secretly because this type of attacker deals with confidentiality and sensitivity in terms of time[19].
- Attempting to steal data, where the attacker, after penetrating the manager's mail account, requests sensitive information from the employee about other employees, especially those working in the financial transactions department, to exploit it for his benefit in financial attempts.

5. How a bec attack works

As shown in Fig. 4 [7], in the beginning, the attacker determines the target. Where, after identifying the target organization, it collects its information through multiple sources, such as data on publicly available social media channels, as well as phone calls to establish a reliable contact or message. After collecting the data, the attacker tries to establish a relationship with the victim who has access to the financial accounts of the organization. Often the relationship-building messages seem real and are sent from a trusted source like the CEO or CFO. This process will likely take place for some time as a week until trust is built between the vic-

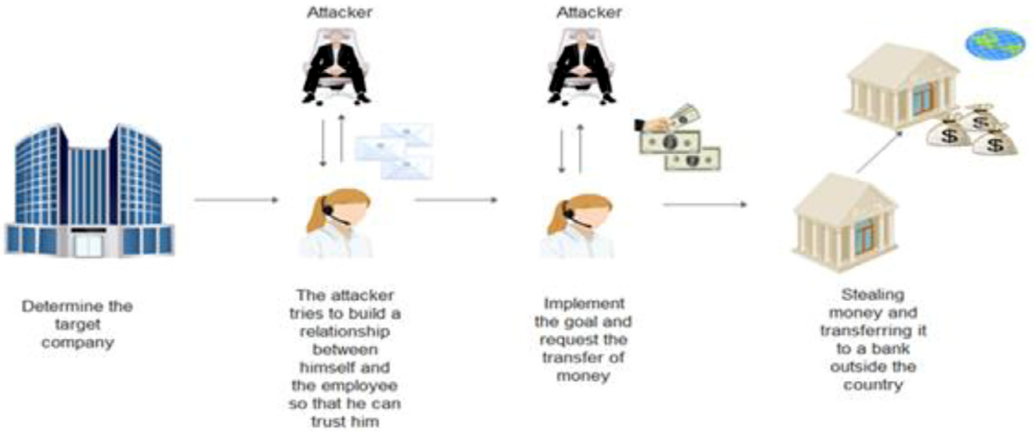

Attacker
Attacker
Determine the target company
The attacker tries to build a relationship between himself and the employee so that he can trust him
Implement the goal and request the transfer of money
Stealing money and transferring it to a bank outside the country

Fig 4. working of BEC attack [7].

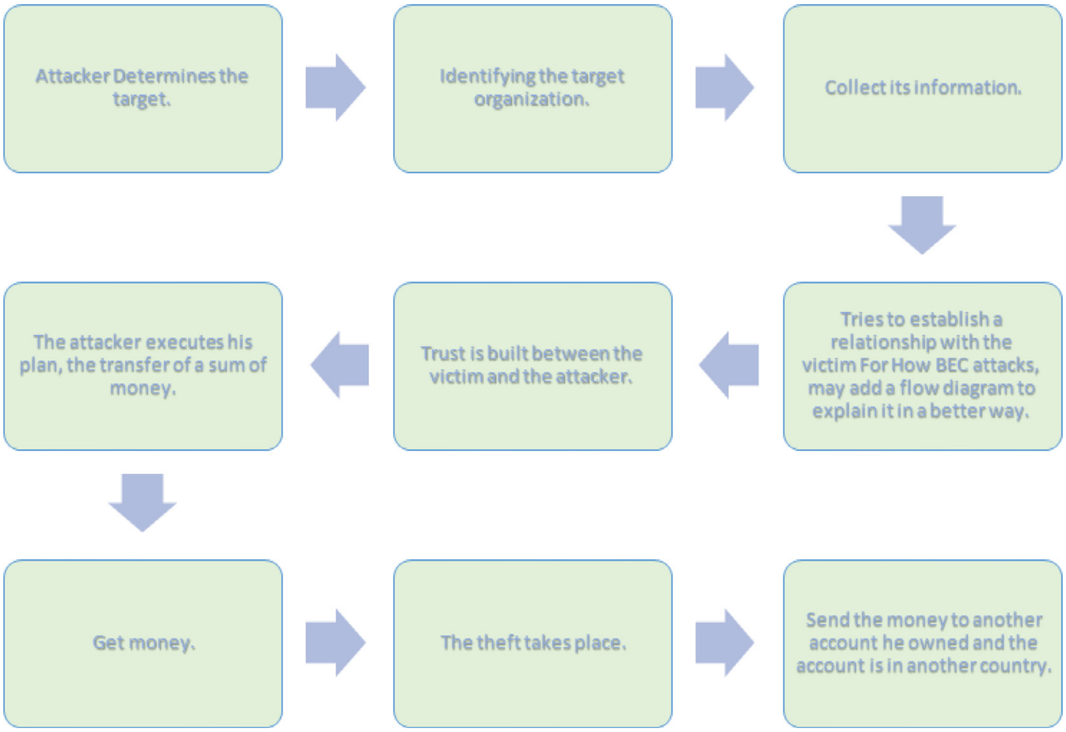

Attacker Determines the target.
Identifying the target organization.
Collect its information.
Tries to establish a relationship with the victim For How BEC attacks, may add a flow diagram to explain it in a better way.
Trust is built between the victim and the attacker.
The attacker executes his plan, the transfer of a sum of money.
Get money.
The theft takes place.
Send the money to another account he owned and the account is in another country.

Fig. 5. Flow diagram of steps to implement BEC attacks.

tim and the attacker. After these two actions, the attacker executes his plan or goal. Where he requests a secret and urgent transfer of a sum of money from the victim to his account. Often this amount is close to the sums that are being circulated so that the request is not compromised, and it is also required to be a purchase among them, and he is unable to contact him as he is in a meeting, for example, or on the plane. Finally, the theft takes place. Urges the attacker to control the money that he received and send it to another account he owned and is mostly unknown, the account is in another country. This type of attack will be discovered after some time as the attacker-controlled the money and the company signed the attack [228].Fig. 5 illustrates these steps in brief.

6. Detection of BEC attack

Below we explain some indications and signs of BEC as classified by the FBI [3]:

- Unexplainable urgency [23].
- Last-minute shifts in wire guidance or payment records for receivers.
- Last-minute shifts in contact channels or email account addresses that have been developed.
- Communications are rendered available via email and an unwillingness to connect via phone or online voice/video channels.
- Demands for advanced service payment if not previously needed.
- Requests from workers to update details on direct deposits.

7. Methods of protection against bec attacks

Many companies have been exposed to this type of fraud and lost very high sums of money, but some of these companies were able to detect and frustrate this fraud in the last moments before it occurred. The insurance firm that deals in mergers and acquisitions of high-value firms were the casualty of a data leak. The business almost found itself as the gateway for complex theft, despite undertaking frequent workforce training and ensuring a high standard of protective safety measures. The assault tried to pressure one of its customers into paying £ 300,000 into a replacement bank account, owing about two unpaid invoices. Fortunately, before any transfers were made, the attack was foiled-a diligent and watchful team member of the client firm had insisted on requesting verbal clarification of the substitution banking information provided-the company was eager to consider the nature of the breach and how to defend against future attacks. Consequently, it sought the assistance of a specialized computer protection firm to perform a full forensic investigation and offer help for remediation [11].

AFGlobal corporation stated a loss of $ 480,000 after an email fraud that impersonated the CEO and tricked the company's accountant to move the money to a bank in China. Where the attacker asked the accounting manager to communicate with him, where the attacker wrote in the message that this content is strictly confidential and has priority over other tasks that must be carried out as soon as possible. Where he requested that communication be only via e-mail and not speak with anyone else about this message, as the attacker requested to transfer a sum of money for 480 thousand dollars as soon as possible to an account in China, and after the transfer, communication between them was only after days, as the attacker told the accounting director The amount has arrived and an additional 18 million dollars must be transferred. . At this moment, the CEO's account became suspicious for the accounting manager, as he told the security team about this process, and the company tried to retrieve the amount, but it was too late as it could not retrieve it because the attacker emptied his account of money and closed it immediately after receiving the money[12].

For this reason, one of the most important steps in protection is to train and educate employees on a permanent and continuous basis for such types of fraud, as described in the theoretical methods.

After learning about this type of fraud and knowing how it occurs in this part, we will explain some methods that help to prevent this type of fraud, whether it is theoretically and technically Because the presence of one of these methods is not sufficient to prevent this kind of fraud.

A. Theoretical methods

- Continuous employee training: Train workers to detect and report an assault and be able to respond immediately. It's not a question of whether an assault is going to sneak in, it's a question of how much. To do your danger hunting, make sure to use surveillance resources as well [524]. Growing the training level for workers accountable for wire transfers and concentrating on teaching them on BEC processes such as executive impersonation and computer protection [10]. Since social engineering is such a crucial factor in these schemes, it is important to increase the consciousness of workers of how this form of fraud works [6]. And so, learning is the first line of protection for an organization. Strengthening knowledge alone would not do the job [6].
- Defining policies: Establish internal regulations Establish policies and guidelines requiring special protections for wire transfer transfers and other financial transactions. Prohibit email requests and other cash transfers for orders. Ensure that the approval process requires several persons to be present [5]. A basic regulation whether it is the executive director or the person responsible for financial transfers and any person in the organization involved in financial transactions for instance that demands, that before someone can adjust the banking information for a transfer, there must be a confirmation phone call with the finance director would also go a long way [625].
- Conducting a wire transfer method risk evaluation to find vulnerabilities that may be abused. To discourage attackers from undertaking BEC attacks, recognize "look-alike" domains, and sign them under the company's name [10].
- Wary of any last-minute modifications to wiring directions or account details for recipients [3 26].
- Check any updates and details via the company's contact in the document and do not call the vendor through the email number provided [3].
- Be warning to hyperlinks that could include the real domain name misspellings [3].

B. Technical methods

- Multi-factor authentication: Reviewing processes and practices for the order, initiation, and acceptance of wire transfers. Phone calls to company-registered numbers can check email requests. Require two staff to accept wire requests and authenticate the identity of the receiver before issuing the wire [3].
- Prevent automated email delivery to foreign accounts [3].
- For messages originating from outside the organization, install an email banner [3].
- Ban old email protocols that can be used to bypass multi-factor authentication, including POP, IMAP, and SMTP [3].
- Ensure all mailbox login modifications and configurations are recorded and maintained for 90 days [3].
- Allow warnings, such as international logins, for suspicious behavior [3].
- Allow protection features, including anti-phishing and anti-spoofing policies, that block phishing emails [3].
- Show workers how to understand executive impersonation. Instruct users. Be sure to point out that a URL or an attachment is not necessarily required for phishing attacks and warn them to double-check email addresses and pay attention to odd requests [5].
- Implement DMARC authentication to defend against hackers spoofing your email domain in their impersonation attacks, set up DMARC authentication. Reports from DMARC include insight and documentation of how and how the email domain is used [5].
- Using machine learning Don't focus exclusively on conventional technology for email security, since most organization email compromise attacks are planned to circumvent gateways. Machine learning technology can analyze internal emails to construct a model of the normal contact of each person. Using this knowledge for attack estimation and identification [5].
- perform encrypted / secure member email correspondence [4].

8. Conclusion

Email fraud and BEC attacks, especially, have continued to grow, develop, and increase over the past few years. BEC is considered one of the most dangerous email threats to organizations and individuals as it costs very large financial losses. This threat or danger is expected to develop and spread in the future greatly due to the heavy reliance on technology at work, so organizations must fully prepare to confront and prevent this threat in terms of educating employees with such a threat, training them an ongoing, and providing assistance software to discover and mitigate its occurrence. In this paper, discussed the concept of BEC attacks, its types, how it occurs, and some case study is illustrated, in addition to present the methods to detect, to avoid, and to prevent BEC, and offer solutions based on some studies.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] Aviv, S., Levy, Y., Wang, L. and Geri, N., 2019. An expert assessment of corporate professional users to measure business email compromise detection skills and develop a knowledge and awareness training program. ICIS, pp.2,3,6.

[2] D. Zweighaft, Business email compromise and executive impersonation: are financial institutions exposed?, J Invest. Compl. 18 (1) (2017) 1–7, https://doi.org/10.1108/joic-02-2017-0001.

[3] J.C. Archie, S. Turner, T. Wybitul, The pervasive threat of business email compromise fraud – and how to prevent It, Intellectual PropertyTechnol. Law Journal 32 (7) (2020) 1–3.

[4] C. Cross, R. Gillett, Exploiting trust for financial gain: an overview of business email compromise (BEC) fraud, J. Financial Crime 27 (3) (2020) 871–884.

[5] N. Rosenthal, J. and J. Oberly, D., 2020. FBI Warns Companies to Be Vigilant as COVID-19- Themed BEC Scams Continue to Grow. Aspen Publishers Inc, 37(8), pp.6-8.

[6] J. Pringle, Avoiding Business Email Compromise Schemes | Credit Union Times, online Credit Union Times. Available at (2019), <https://www.cutimes.com/2019/07/12/avoiding-business-email-compromise-schemes/> [Accessed 29 November 2020].

[7] A. Campbell, Report: Defending Against Business Email Compromise Attacks, [online] Journey Notes. Available at (2020), <https://blog.barracuda.com/2019/11/21/report-defending-against-business-email-compromise-attacks/> [Accessed 29 November 2020].

[8] A.A. Ubing, S. Kamilia, A. Abdullah, N.Z. Jhanjhi, M. Supramaniam, Phishing website detection: An improved accuracy through feature selection and ensemble learning, International Journal of Advanced Computer Science and Applications (IJACSA) 10 (1) (2019), https://doi.org/10.14569/issn.2156-557010.14569/IJACSA.2019.0100133.

[9] S. Myojin, N. Babaguchi, A logical consideration on fraudulent email communication, Artificial Life and Robotics 25 (3) (2020) 475–481.

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

[11] M. Nicholls, The Rise Of Sophisticated BEC Scams In The Finance Industry, [online] Finance Digest. Available at (2020), <https://www.financedigest.com/rise-sophisticated-bec-scams-finance-industry.html> [Accessed 28 November 2020].

[12] MailSurance. 2020. Case Studies In Business Email Compromise (BEC) | Mailsurance. [online] Available at: <https://www.mailsurance.com/press/case-studies-in-business-email-compromise-bec> [Accessed 28 November 2020].

[13] A. Cidon L. Gavish I. Bleier N. Korshun M. Schweighauser A. Tsitkin High Precision Detection of Business Email Compromise USENIX Association online 2019 1291 1307 Available at: <https://www.usenix.org/conference/usenixsecurity19/presentation/cidon> [Accessed 28 November 2020]

[14] B. Opazo, D. Whitteker, C. Shing, Email Trouble: Secrets of Spoofing, the Dangers of Social Engineering, and How We Can Help, in: International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC-FSKD 2017), IEEE, China, 2017, pp. 2812–2817.

[15] K. Liao, The state of business email compromise Q1 2020: Attacks shift from the C-suite to finance - Abnormal security, [online] Abnormal Security. Available at (2020), <https://abnormalsecurity.com/blog/the-state-of-business-email-compromise-q1-2020-attacks-shift-from-the-c-suite-to-finance/> [Accessed 29 November 2020].

[16] E. Reiser, Report: Abnormal Security's Q2 2020 Quarterly BEC Report, [online] Info.abnormalsecurity.com. Available at (2020), <https://info.abnormalsecurity.com/Q2-2020-Quarterly-BEC-Report.html> [Accessed 29 November 2020].

[17] Reiser, E., 2020. Quarterly BEC Report Q3 2020. [online] Info. abnormalsecurity.com. Available at: <https://info.abnormalsecurity.com/rs/231-IDP-139/images/AS_Qtrly_BEC_Report_Q3_2020.pdf> [Accessed 29 November 2020].

[18] Camillo, M., Avery, K. and Martinez, J., 2020. Cyber Claims: GDPR And Business Email Compromise Drive Greater Frequencies. [online] Aig.co.uk. Available at: <https://www.aig.co.uk/content/dam/aig/emea/regional-assets/documents/aig-cyber-claims-2019.pdf> [Accessed 30 November 2020].

[19] K. Hussain, S.J. Hussain, N. Jhanjhi and M. Humayun, SYN Flood Attack Detection based on Bayes Estimator (SFADBE) For MANET, 2019 International Conference on Computer and Information Sciences (ICCIS), Sakaka, Saudi Arabia, 2019, pp. 1-4, doi: 10.1109/ICCISci.2019.8716416.

[20] D. Pienta, J.B. Thatcher, A. Johnston, Protecting a whale in a sea of phish, J. Inform. Technol. 35 (3) (2020) 214–231.

[21] K. Bakarich, D. Baranek, Something phish-y is going on here: A teaching case on business email compromise, Current Issues in Auditing 14 (1) (2019) A1–A9.

[22] Buo, S., 2020. An Application Of Cyberpsychology In Business Email Compromise. [online] arXiv.org. Available at: <https://arxiv.org/abs/2011.11112> [Accessed 30 November 2020].

[23] A. Ecclesie Agazzi Business Email Compromise (BEC) And Cyberpsychology [online] NASA/ADS. Available at 2020 <https://ui.adsabs.harvard.edu/abs/2020arXiv200702415E/abstract> [Accessed 30 November 2020]

[24] D. Lohrmann, Scammers target legacy tech: Three ways to stop business email compromise, Government Technol. 30 (5) (2017) 48.

[25] Ferraro, M., 2019. YOU'VE GOT FRAUD. Claims, 67(7), pp.22-24.

[26] C. Taylor, FinCEN advises financial institutions on fighting email compromise fraud, Tellervision 1471 (2016) 1–4.

[27] M. Foreman, CEOs under fire from email fraud, Credit Control 37 (5/6) (2016) 19–21.

[28] M. Weinstein, Business email compromise and wire fraud: how to protect your clients and firm in the year ahead, [online] Business Source Ultimate. Available at (2017), <http://www.penton.com/> [Accessed 30 November 2020].

[29] A. RICE, Business email scams move closer to advanced threats, TechTarget 20 (3) (2018) 11–16.

[30] D. Salierno, S. Steffee, Cybercrime: Email fraud, Instit. Intern. Auditors (IIA) 77 (2) (2020) 13.