electronics

MDPI

Review

Business Email Compromise Phishing Detection Based on Machine Learning: A Systematic Literature Review

Hany F. Atlam [1,2,*] and Olayonu Oluwatimilehin [1]

[1] School of Computing and Engineering, University of Derby, Derby DE22 3AW, UK
[2] Computer Science and Engineering Department, Faculty of Electronic Engineering, Menoufia University, Menouf 32952, Egypt
* Correspondence: h.atlam@derby.ac.uk

Abstract: The risk of cyberattacks against businesses has risen considerably, with Business Email Compromise (BEC) schemes taking the lead as one of the most common phishing attack methods. The daily evolution of this assault mechanism's attack methods has shown a very high level of proficiency against organisations. Since the majority of BEC emails lack a payloader, they have become challenging for organisations to identify or detect using typical spam filtering and static feature extraction techniques. Hence, an efficient and effective BEC phishing detection approach is required to provide an effective solution to various organisations to protect against such attacks. This paper provides a systematic review and examination of the state of the art of BEC phishing detection techniques to provide a detailed understanding of the topic to allow researchers to identify the main principles of BEC phishing detection, the common Machine Learning (ML) algorithms used, the features used to detect BEC phishing, and the common datasets used. Based on the selected search strategy, 38 articles (of 950 articles) were chosen for closer examination. Out of these articles, the contributions of the selected articles were discussed and summarised to highlight their contributions as well as their limitations. In addition, the features of BEC phishing used for detection were provided, as well as the ML algorithms and datasets that were used in BEC phishing detection models were discussed. In the end, open issues and future research directions of BEC phishing detection based on ML were discussed.

Keywords: business email compromise (BEC); email phishing; phishing detection; machine learning (ML); systematic literature review

check for updates

Citation: Atlam, H.F.; Oluwatimilehin, O. Business Email Compromise Phishing Detection Based on Machine Learning: A Systematic Literature Review. *Electronics* **2023**, *12*, 42. https://doi.org/10.3390/electronics12010042

Academic Editor: Suleiman Yerima

Received: 20 November 2022
Revised: 15 December 2022
Accepted: 19 December 2022
Published: 22 December 2022

1. Introduction

The popularity of Internet-based public resources, such as cloud computing, social networks and online money processing, has significantly raised the danger of cyberattacks against enterprises. Since email has become one of the effective worldwide standards for commercial communication, cybercriminals attack email networks to undertake cyberattacks against companies for financial gain [1]. A Business Email Compromise (BEC) attack, often known as a CEO attack, is one of the most significant spear phishing attacks. BEC attacks are defined as sophisticated email phishing schemes that target businesses doing mundane tasks, such as money transfers [1]. Social engineering has shown to be a highly effective component of BEC attacks, which are designed to deceive corporations and their employees throughout the world. According to the Federal Bureau of Investigation (FBI) [2], victims worldwide lost more than USD 26 billion to BEC attacks between June 2016 and July 2019. In 2018, almost AUD 60 million was reported lost in Australia using this strategy. In addition, the United States (39%), the United Kingdom (26%), Australia (11%), Belgium and Germany (3%), Canada, the Netherlands, Hong Kong, Singapore, and Japan (2%), were the top 10 victim nations for BEC attacks in 2018–2019.

The reason why cyberattacks are becoming increasingly prevalent is that launching a cyberattack is simpler, cheaper, and less dangerous than launching a physical attack. The only requirements for committing a cybercrime are an Internet connection and a computer. In addition, the anonymity given by the Internet makes it difficult to trace and find attackers and bring them to justice [3].

BEC attacks are prevalent and have not been detected by conventional defence strategies, such as spam filters. Without a harmful payload, BEC attacks are difficult to detect with conventional screening equipment. BEC attacks are gaining popularity due to their effectiveness and difficulties in monitoring or detecting them [1]. Unlike other attacks using banking trojans or other forms of criminal ransomware, which may require a higher level of technical skill to execute, BEC attacks do not require an exceptionally high level of technical skill to execute; other than having the first name, last name, and email address of whoever they wish to address the email to, they do not need much analysis [2]. Hence, more investigation on BEC attacks is required to identify possible solutions for them.

BEC is a relatively new and fast-evolving attack in the phishing domain with less than ten years since its first identification in 2013 by the FBI. The novelty of this type of attack has led to several challenges regarding how much of its attack pattern and structure has been fully understood by experts to build an effective phishing detection model. In addition, how to ensure the resources needed to identify a BEC attack and the measure used to detect it do not become outdated due to the fast-changing pattern of this type of attack is important. These challenges make detecting BEC attacks using conventional defence strategies a very difficult task to achieve. To overcome these challenges, Machine Learning (ML) has been proposed by various researchers as an effective way to detect BEC attacks in a timely manner. Instead of using conventional phishing detection techniques that detect and block emails based on their origin, as well as applying common block listed locations which require significant time and effort to maintain, ML-based phishing detection techniques can identify and even predict advanced attacks by analysing large datasets to spot similarities, correlations, and trends. For instance, ML can be used to build a phishing detection model based on profiles where ML can be used to build a profile by analysing emails using features such as date, time, geo-location from where a person is accessing emails, relation graph which captures with whom the person interacts, etc. Then, the ML-based model will scan every incoming email against the profile and raise an alert for BEC in case of any deviation. ML-based techniques leveraged by modern email security platforms have become more effective, in which most techniques can detect around 98% of advanced phishing attacks [4].

This paper aims to provide a comprehensive systematic literature review that investigates and evaluates the state of the art of BEC phishing attacks, one of the primary attack domains that has a significant impact on organisations and has resulted in the loss of billions every year. Based on the selected search strategy, 38 articles out of 950 were chosen for further analysis. Out of the collected and analysed articles, articles were selected based on the manner of detection using ML algorithms, and additional assessment was obtained from the articles to comprehend what feature criteria were used for detection. In addition, a summary of the selected papers' contributions was provided. Compared to other surveys, to the best of the authors' knowledge, this is the first work to provide a systematic literature review of BEC phishing attacks. Most existing surveys focus on providing a general investigation and discussion of phishing attacks without focusing on BEC attacks and how creating effective BEC phishing detection models is now a necessity for various organisations around the world. This paper also provides a detailed discussion of BEC phishing attacks to allow researchers to have a complete overview of this type of attack, its detection methods, features, and challenges, which can allow them to develop optimised and sustainable techniques for detecting it effectively.

The contribution of this paper can be summarised as follows:

- Investigating and reviewing recent research on BEC detection by highlighting the merits of each study.
- Identifying common ML algorithms for the development of BEC phishing detection models.

- Determining common features used in BEC phishing detection models.
- Identifying common datasets used in BEC phishing detection models.
- Presenting challenges and future research directions of BEC phishing attacks.

The rest of the paper is organised as follows. Section 2 presents an overview of BEC attacks; Section 3 describes the research methodology used to produce the systematic literature review; Section 4 describes the analysis of data; Section 5 describes how this systematic review answers suggested research questions; Section 6 presents challenges and future research directions; and Section 7 is the conclusion.

2. An Overview of BEC Attack

Phishing is a type of email-based fraud and attack. Phishing happens when an attacker sends a bogus email that seems to originate from a reputable and approved source. The objective of the message is to deceive users into downloading malware on their devices and divulging sensitive information. Spear phishing is a targeted kind of phishing. Phishing and spear phishing both utilise email to target victims, but spear phishing delivers a personalised message to a particular individual. Before sending the email, the criminal searches the interests of the intended victim. It is important to understand that phishing emails nowadays are mostly used to acquire credentials [3].

BEC is one of the most significant spear-phishing attacks. This section provides an overview of this type of BEC attack to highlight the BEC lifecycle, types, and techniques that are used for detecting it.

2.1. BEC Attack

BEC is a form of attack that has evolved over the years from a simply compromised vendor email to requests for sensitive information, such as by targeting the real estate sector, and fraudulent requests for large amounts of gift cards. For a BEC attack to be successful, hackers first need to gain access to legitimate vendor email accounts. The most common method for accomplishing this is via phishing emails sent to the company's staff. The credentials of a worker who unknowingly lets themselves be compromised are a springboard for an attack [3].

The FBI created the term "business email compromise", or in short BEC, in 2013 when it first began tracking this issue. However, the strategy might be regarded as the natural progression of huge spamming campaigns that came before it. These promotions originated with what is now commonly referred to as Nigerian prince or lottery schemes. These email frauds were noticeable for their lack of professionalism—misspellings, grammatical errors, and implausible tales—and were easy to recognise and disregard. However, the offenders swiftly acquired technological expertise and today deploy some extremely sophisticated approaches [4].

2.2. BEC Lifecycle

BEC attacks are usually harder to spot than other phishing attacks, as they can play out in various ways. Figure 1 shows common steps for performing a successful BEC attack [4].

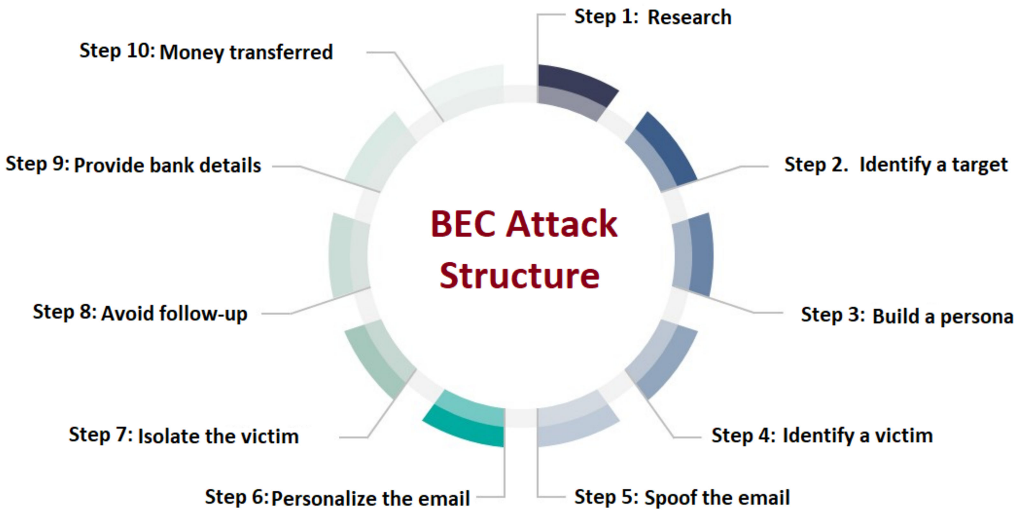
BEC Attack Structure
Step 1: Research
Step 2. Identify a target
Step 3: Build a persona
Step 4: Identify a victim
Step 5: Spoof the email
Step 6: Personalize the email
Step 7: Isolate the victim
Step 8: Avoid follow-up
Step 9: Provide bank details
Step 10: Money transferred

Figure 1. Common steps of performing a BEC attack.

The description of each step is as follows:

- Step 1—Research: Potential victims' vulnerabilities and openings are scouted by attackers.
- Step 2—Identify a target: Based on the research, the criminals decide what angle they will try to exploit and which organisation they will target.
- Step 3—Build a Persona: Through a web search, the criminals can identify board members in the target organisation.
- Step 4—Identify a victim: Next, they look for an individual at the target organisation whom they want to trick.
- Step 5—Spoof the email: The attack starts with an email that appears to come from the senior leader. The crooks first spearfish the executive to get their credential, then log in as them to send their email.
- Step 6—Personalise the email: The attacker puts all their research and persona-building work to good use, crafting an email that appears to come from the senior leader.
- Step 7—Isolate the Victim: Isolation is a popular technique to pressure the victim and stop them from checking with others.
- Step 8—Avoid Follow-up: The attacker does not want the victim checking in with the senior leader, so they discourage the victim by making the senior leader seem unavailable, such as by saying they are out of the office.
- Step 9—Provide bank details: The bank account detail is one of the attacker's biggest expresses, so they will only share after they have hooked the victim with their spoofed email.
- Step 10—Money transferred: The game is over; the money has been sent to the attacker and will never be seen again. Soon, someone will notice a big hole in the bank account, and that is when the alarm will go on.

2.3. Types of BEC Attacks

According to the FBI [4], there are five types of BEC attacks which include the following:

1. Email Account Compromise: This attack is targeted at small firms that use email to organise their financial transactions. The specifics of a recent transaction can be gleaned by breaking into an employee's email account and stealing the invoice. Attackers call a vendor and explain the situation, persuading the vendor that the final payment could not be processed. A new account, which the scammers would have set up to steal the money, is gently requested by them [4].

2. Lawyer Impersonation: This type of attack is fraud committed mostly against major corporations and the law firms that serve them. Attackers pose as a lawyer for a client of the company's law practice and ask for a quick transfer for the payment of an outstanding debt. To protect the transaction from being leaked, they convince the employee that the subject is private by making clear that they are demanding that the employee should not discuss it with anyone. Oftentimes, attackers plan it towards the conclusion of the work week to put the employee under more pressure to respond swiftly [4].
3. Data Theft: As part of a BEC attack, a top executive's email account is compromised and a request for critical company information is made. This is an example of a BEC attack that does not include any money laundering. It is often a prelude to a far more serious cyberattack, as this type of attack focuses on finance and human resources [5].
4. Vendor Email Compromise: It is common in businesses with overseas vendors. Attackers assume the role of vendors, demand payment for a fictitious invoice, and then transfer the funds to a fake account [4].
5. CEO Fraud: Attackers pretend to be a company's CEO or executive. As the CEO, they ask a worker in the accounting or finance division to transfer money to an account under the control of the attackers.

2.4. Phishing and BEC Techniques

This section highlights techniques of phishing attacks generally and BEC attack specifically.

2.4.1. Phishing-Related Techniques

Typically, a phishing attack includes sending an email that contains a spoof URL link that leads to a web page. The following are common phishing techniques:

- Direct Link: Links are usually accessible in the body of the email. In addition, they may contain hidden links or image links that lead to phishing or another dangerous website [6].
- PDF Files: Email attachments that include a PDF file are a typical phishing method because they make the recipients believe that the attached document is essential, such as an eye-catching business proposal or an urgent invoice. Even if the PDF file does not include any malicious code, the material inside the PDF file might be crafted to direct the recipients to phishing sites [7].
- HTML: The phishing email might also include a malicious HTML file. Even though HTML files are rarely utilised in commercial transactions, these attachments can nonetheless deceive unwary users. The target will be sent to a malicious URL if he or she clicks and downloads the attachment [8].
- File-hosting Services: One of the most prevalent methods used by attackers to trick users into visiting phishing sites is the misuse of file-hosting services [9].
- Malware-related Techniques: Keyloggers and Remote Access Tools (RATs) are the most utilised malware for BEC. Malware, unlike phishing attempts, may grab all computers' saved login credentials before delivering them to the attackers. Hacking forums are flooded with new keyloggers and RATs, offering cybercriminals easy access to sophisticated yet undetectable malware. BEC attacks have been plagued by a wide range of software, the most frequent of which being adware including AgentTesla, CyborgLogger, DarkComet, DiamondFox, Dracula Logger, iSpy Keylogger, Knight Logger, and LuminosityLink [10].

2.4.2. BEC Techniques

- **Spoofed BEC Messages:** The email domain may be manipulated to make the email appear to be legitimate in this method. Email header spoofing is used by attackers to produce fraudulent emails that appear to originate from a legitimate source. In the "From" address area, they use the true domain of the target company [4].

- **BEC Basic Header Trickery:** Another tactic adopted by attackers is to use a faked organisation's true domain in the "From" address box. Adding another domain to the "Reply-To" address box tricks the users into thinking they have received a reply. A reply to a field controlled by the attacker results in a reply being sent back to the attacker [1].
- **BEC Business Domain Similarity Attacks:** The "From" domain used in this attack is the same as the target domain. This gives the appearance that emails are coming from a higher authority and are being sent to employees asking for a quick response. To a foreign client or supplier, it may be necessary to make an immediate transfer of funds [2].
- **Executive Name Forgery:** In an attack known as ID Spoofing, the hacker inserts a fake executive name into the "From" box of an email. This title-spoofing technique takes advantage of the display label to spoof the names of corporate executives (CxOs) [2].
- **BEC Encoded Message Attack:** To avoid being detected by email gateways, BEC attackers sometimes utilise encoding ploys that alter the characters in the message. When a BEC message is opened in the email account of a client, it seems to be a regular email. A hex editor scan, on the other hand, reveals the real colours of the image [4].
- **BEC Attacks using Long Scenario to Lure Victims:** Using long, individualised emails to request sworn confidentiality from recipients because of legal repercussions of a vital business necessity is another typical practice. Law firms are frequently mentioned in these emails to remind their receivers that they need to follow legal and commercial requirements carefully in order not to divulge confidential information. The attacker will next seek access to the company's bank accounts and financial records, which they will study to make further demands for money transfers [5].
- **BEC Emails Demanding Gift Cards:** Criminals request iTunes, Amazon, and Walmart gift cards from their victims. Instead of requesting a wire transfer, this attack asks for the credentials of a gift certificate that the victim has received in person. It uses a standard message structure to demand first priority [4].
- **BEC Attackers Targeting Schools and Academic Institutes:** Emails from the school's principal or top management asking for wire transfers or gift vouchers from school workers are another common BEC technique [4].

2.4.3. Feature Selection Techniques

When developing an ML-based phishing detection model in the real world, it is usually never the case that all variables in the dataset are significant. Adding duplicate variables diminishes the model's capacity for generalisation and affects the overall accuracy of the detection model. Additionally, when more variables are added to the model, its total complexity grows. According to the Law of Parsimony of 'Occam's Razor,' the optimal answer for a problem is the one that requires the fewest assumptions. Thus, feature selection becomes an essential component in ML-based model development [9].

Feature selection is the method of reducing the input variables of a ML-based model by using only relevant data and getting rid of noise in the data. Its main goal is to clean up a model by getting rid of irrelevant or unnecessary data. Due to the complexity of some predictive modelling issues, considerable memory is often needed during model creation and training. In addition, certain models' functionality can deteriorate if the input variables are not pertinent to the target variable. In ML, the strategies for feature selection are categorised into two main categories: supervised and unsupervised. The supervised feature selection methods are applied to labelled data to discover the most important variables for improving the performance of supervised models. In other words, they use the target variables to identify the variables which can increase the efficiency of the model. Unsupervised feature selection methods are applied to unlabelled data in which the outcome is not considered while making the feature selection [10]. Figure 2 shows the categories of feature selection methods.

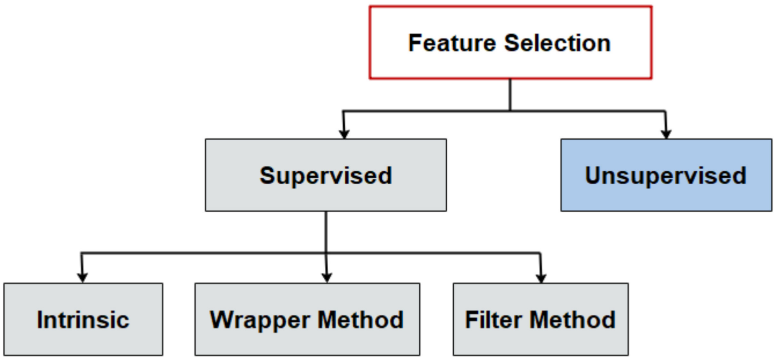

Figure 2. Feature selection methods.

The supervised methods are further divided into three methods, including filter, wrapper, and intrinsic methods [10,11].

- **Filter Method**: In this method, features are eliminated according to how they correlate with the output. Correlation is used to determine if the features are positively or negatively correlated to the output labels and then the features are dropped accordingly. Examples include Fisher's Score, Variance Threshold, Correlation Coefficient, Chi-Square Test, etc.
- **Wrapper Method**: Wrappers need a way to explore the space of all possible subsets of features, evaluating their quality by learning and evaluating a classifier with that subset of features. The feature selection procedure is determined by a particular ML algorithm that employs a greedy search strategy by comparing all potential feature combinations to the evaluation criterion. Wrapper approaches often produce more accurate predictions than filter methods. Wrapper methods include Forward Feature Selection, Backward Feature Elimination, Exhaustive Feature Selection, etc. [12].
- **Intrinsic Method**: This method, also called the embedded method, combines the advantages of wrapper and filter methods by including feature interactions while retaining an acceptable computing cost. This approach is iterative in the sense that it takes care of each iteration of the model training process and meticulously extracts the features that contribute the most to training for each iteration. Examples include Random Forest Importance and LASSO Regularisation (L1).

2.4.4. Evaluation Metrics for BEC Detection

Determining the effectiveness of BEC phishing detection models is significant to compare different models and identify the most effective model for each context. Based on numerous studies reviewed in the literature [5,9,10], the effectiveness of BEC phishing detection models is computed based on four main evaluation metrics, including accuracy, precision, recall, and F-measure. A description of how these evaluation metrics is computed is discussed below:

- **True Positive (TP):** This represents the percentage of phishing emails in the training dataset that are correctly classified by a phishing detection model. Formally, if the number of phishing emails in the dataset is denoted by *P* and the number of correctly classified phishing emails by the phishing detection model is denoted by *NP*, the formula of *TP* is as follows:

$$TP = \frac{NP}{P} \tag{1}$$

- **True Negative (TN):** This represents the percentage of legitimate emails that are correctly classified as legitimate by a phishing detection model. If we denote the number of legitimate emails that are correctly classified as legitimate as *NL* and the total number of legitimate emails as *L*, the formula of *TN* is as follows:

$$TN = \frac{NL}{L} \tag{2}$$

- **False Positive (FP):** This is the percentage of legitimate emails that are incorrectly classified by a phishing detection model as phishing emails. If we denote the number of legitimate emails that are incorrectly classified as phishing as *Nf* and the total number of legitimate emails as *L*, the formula of *FP* is as follows:

$$FP = \frac{Nf}{L} \tag{3}$$

- **False Negative (FN):** This represents the percentage of the number of phishing emails that are incorrectly classified as legitimate by a phishing detection model. If we denote the number of phishing emails that are classified as legitimate by the algorithm as *Npl* and the total number of phishing emails in the dataset is denoted as *P*, the formula of *FN* is as follows:

$$FN = \frac{Npl}{P} \tag{4}$$

Using TP, TN, FP, and FN, the four evaluation metrics, including accuracy, precision, recall, and F-measure, can be computed as follows:

- **Accuracy**: It represents the average number of successfully categorised emails throughout the entire dataset using the following formula:

$$Accuracy = \frac{TP + TN}{TP + FP + FN + TN} \tag{5}$$

- **Precision**: It measures the exactness of a classifier, i.e., what percentage of emails that the classifier has labelled as BEC phishing are actually BEC phishing emails, and it is represented by this formula:

$$Precision = \frac{TP}{TP + FP} \tag{6}$$

- **Recall:** It measures the completeness of a classifier's results, i.e., what percentage of phishing emails the classifier has labelled as phishing, and it is represented by this formula:

$$Recall = \frac{TP}{TP + FN} \tag{7}$$

- **F-measure:** This is also known as $F1$ score and is defined as the harmonic mean of Precision and Recall, and it is calculated based on this formula:

$$F1 - Score = \frac{2TP}{2TP + FP + FN} \tag{8}$$

3. Research Methodology

The purpose of a systematic literature review is to define, analyse, and interpret all available research relevant to a research topic, a specific subject, or a set of interesting occurrences. While several experts have offered solutions to detecting BEC attacks, the threat environment is expanding and becoming more dangerous despite their efforts. This systematic literature review investigates existing BEC attack techniques and detection methods, as well as various studies presented by researchers using different ML algorithms employed in the detection process and these studies' conclusions.

Conducting a systematic literature review consists of five stages, as shown in Figure 3. The objective of the first stage is to formulate the research questions that the current review will answer. This is followed by determining the inclusion and exclusion criteria to ensure that the selected articles are the best and most pertinent concerning the research objectives. The third stage is to specify which research databases will be searched to find relevant articles. In the fourth stage, the findings are analysed, and, in the fifth stage, the outcomes of each study topic are discussed.

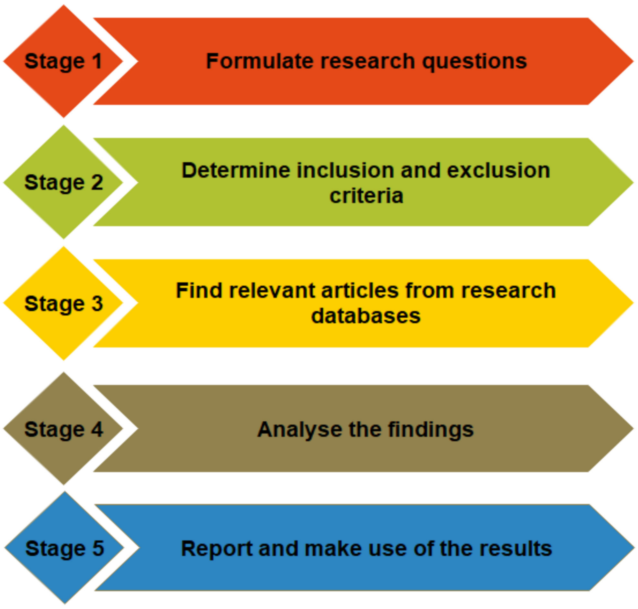
Stage 1
Formulate research questions
Stage 2
Determine inclusion and exclusion criteria
Stage 3
Find relevant articles from research databases
Stage 4
Analyse the findings
Stage 5
Report and make use of the results

Figure 3. Stages of conducting a systematic literature review.

This methodology was utilised to allow readers to understand the stages used to complete this literature review systematically. Before beginning to evaluate many sources, we defined our research questions so that the review would be more focused. Next, the selection criteria were used to narrow down the retrieved publications to those relevant to the study's objectives. The digital libraries that were used to compile these articles are also offered as data sources. Article selection based on relevance was also covered. The presented methodology offers various benefits to show the steps taken by researchers to reach their study's intended results.

Although this methodology has been used in several systematic literature studies, there are some limitations, including the fact that it narrows the focus of the review/study and, hence, may not provide readers with all the facts they need to fully understand the subject matter at hand. In addition, data collection was limited to only six sources for collecting relevant publications in our study, which could limit the number of publications reviewed. Although these sources are the most reliable sources identified in various systematic literature studies, this could be considered a limitation as not all sources were investigated to identify relevant articles related to the study objectives. In addition, this study reviewed only articles published between 2012 and 2022. Although this study provides readers a review of state-of-the-art articles published in the last ten years, the search methodology limits the number of publications that can be reviewed in the study.

3.1. Research Questions

This paper seeks to address the following research questions:

- **RQ1**: What is the most recent and peer-reviewed literature regarding BEC phishing attacks?
- **RQ2**: What are the common ML algorithms used for developing ML-based BEC detection models?
- **RQ3**: What are the common datasets used in creating BEC detection models?

- **RQ4**: What are the conventional features used in developing an effective BEC detection model?

3.2. Inclusion and Exclusion Criteria

Inclusion and exclusion criteria were used to choose the applicable research. The primary purpose of these criteria was to answer the research questions and assure the creation of an effective literature review. The inclusion criteria were as follows:

- Peer-reviewed and scientific papers.
- Relevant to the specific research questions.
- Topic mainly on BEC phishing attack.
- English-language articles.
- Published between 2012 and 2022.

The exclusion criteria were as follows:

- Article concerning all other phishing attacks, including clone attacks, whaling, vishing, etc.
- Unpublished articles, non-peer-reviewed articles, and editorial articles.
- Articles that are not fully available.
- Non-English articles.
- Duplicates of already included articles.

3.3. Data Sources

Digital libraries were used to conduct the searches. The electronic databases used in this systematic literature review included the following:

- IEEE Xplore.
- PubMed.
- Elsevier ScienceDirect.
- Google Scholar.
- ACM Digital Library.
- SpringerLink.

The papers pertinent to the subject and study questions were gathered using keyword searches. The search terms used included the following:

- BEC phishing attack.
- Spoofed BEC messages.
- BEC basic header trickery
- BEC business domain similarity attacks.
- Executive name forgery.
- BEC encoded message attack.
- BEC emails demanding gift cards.

3.4. Selection of Relevant Articles

This step involved choosing relevant and recent studies on BEC phishing attacks among the 950 articles gathered from various online digital libraries. The process of selecting relevant publications was divided into three phases:

- **Phase 1**: Publications found during the search and those already in the collection were sorted using the inclusion and exclusion criteria. The scope of the search was narrowed to include only articles published between 2012 and 2022 that dealt with the topic of BEC phishing attacks.
- **Phase 2**: The titles and abstracts of the articles collected from several digital libraries were reviewed to determine how well they addressed the topic and the questions posed in this research work.
- **Phase 3**: During this stage, we focused on eliminating duplicates among the six digital libraries used for our publication collection.

4. Analysis of Results

The inclusion and exclusion criteria were applied to the collected publications in three phases, as indicated earlier. A total of 887 articles were removed based on the evaluation by simply reading the titles and abstracts and their relevance to the research questions. Furthermore, duplication across various online digital databases (25 publications) was removed, as shown in Figure 4.

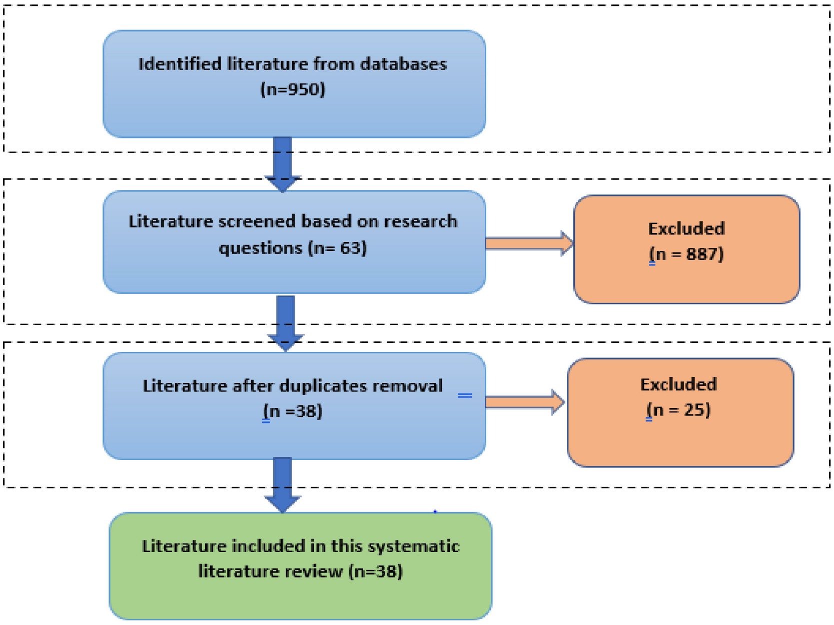
Identified literature from databases (n=950)
Literature screened based on research questions (n= 63)
Excluded (n = 887)
Literature after duplicates removal (n =38)
Excluded (n = 25)
Literature included in this systematic literature review (n=38)

Figure 4. Flow diagram of the search.

The search that was executed in six different well-known online databases enabled us to collect most of the publications that are relevant to BEC phishing attacks. The results of the collected publications from each online database and the resultant number of publications after applying the three selection phases are shown in Table 1. The results show that Google Scholar and IEEE are the richest data sources of publications related to BEC phishing attacks.

Table 1. The number of search results per database after applying the three selection phases.

Data Source	Phase 1	Phase 2	Phase 3
Google Scholar	734	26	17
IEEE Xplore	90	15	10
PubMed	4	2	1
Elsevier ScienceDirect	42	4	2
ACM Digital Library	40	2	1
SpringerLink.	40	14	7
Total	950	63	38

Additionally, the number of publications related to BEC phishing attacks per year is shown in Figure 5. The evidence suggests an upsurge in the study of BEC phishing attacks since 2017. However, many scientists still consider this to be a frontier. Research on BEC attacks has received consistent attention since 2017, as shown by the number of publications in 2017, 2018, 2019, 2020, 2021, and 2022.

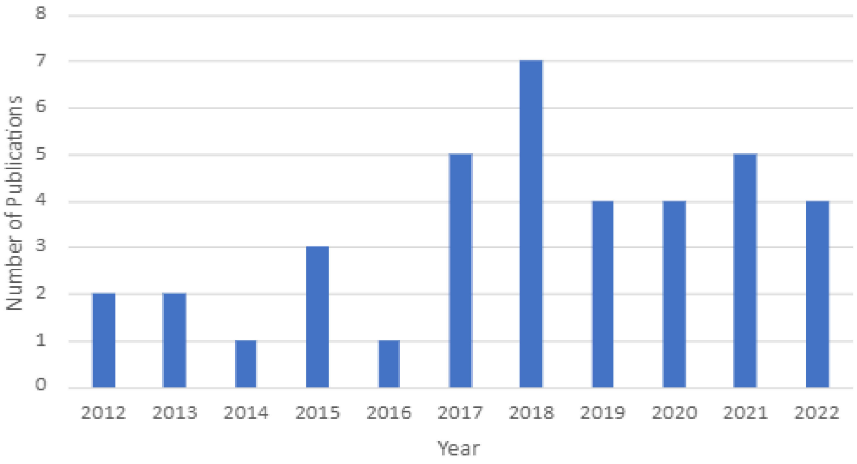

Figure 5. Number of selected articles published per year from 2012 to 2022.

Furthermore, the papers on BEC phishing attacks that were retrieved are separated by year and type (either as a journal or conference publication), as shown in Figure 6. Conference and journal articles both yield similar numbers of outcomes that meet our study objectives. In addition, Table 2 lists the ID, citation, publication category, and publication year for each of the examined articles. All of the papers that were read and retrieved were originally presented at academic conferences or published in scholarly publications.

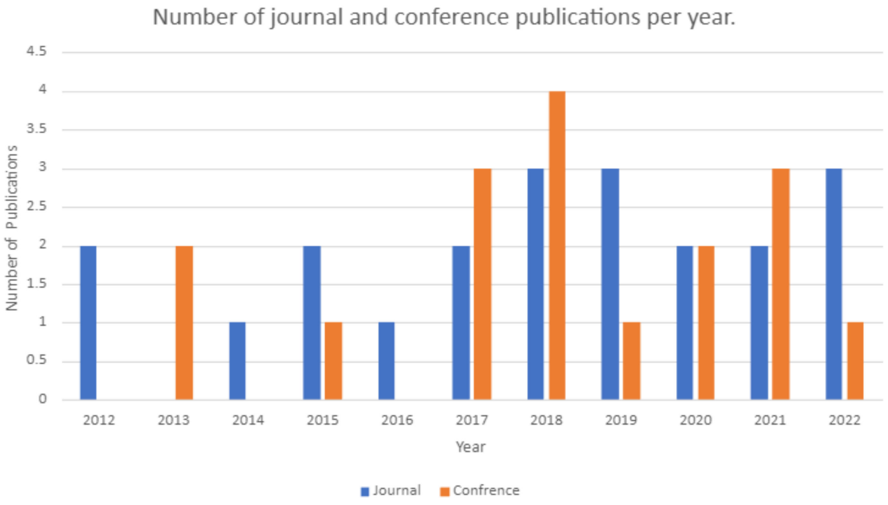

Figure 6. Number of journal and conference publications per year from 2012 to 2022.

Table 2. Retrieved publications that are related to the research questions.

Publication ID	Citation	Publication Type	Publication Year
1	Chakraborty and Mondal [11]	Journal	2012
2	Qasem, Shamsuddin, and Zain [12]	Journal	2012
3	Dhanaraj and Karthikeyani [13]	Conference	2013
4	Shams and Mercer [14]	Conference	2013
5	Laorden et al. [15]	Journal	2014
6	Rathod and Pattewar [16]	Conference	2015
7	Zhu, Dong, and Liu [17]	Journal	2015
8	Daeef et al. [18]	Journal	2015
9	Yasin and Abuhasan [19]	Journal	2016
10	Zweighaft [20]	Journal	2017

Table 2. *Cont.*

Publication ID	Citation	Publication Type	Publication Year
11	Rawal et al. [21]	Journal	2017
12	Zeng [22]	Conference	2017
13	Moradpoor, Clavie, and Buchanan [23]	Conference	2017
14	Niu et al. [24]	Conference	2017
15	Peng, Harris, and Sawa [25]	Conference	2018
16	Baykara and Gurel [26]	Conference	2018
17	Sahoo [27]	Conference	2018
18	Hiransha, Unnithan, and Kp [28]	Journal	2018
19	Singh, Pamula, and Shekhar [29]	Conference	2018
20	El Aassal et al. [30]	Journal	2018
21	Nidhin et al. [31]	Journal	2018
22	George Fomunyam [32]	Journal	2019
23	Oña et al. [33]	Conference	2019
24	Maleki and Ghorbani [34]	Journal	2019
25	Yang et al. [35]	Journal	2019
26	Garces, Cazares, and Andrade [36]	Conference	2020
27	Rendall, Nisioti, and Mylonas [37]	Journal	2020
28	Alam et al. [38]	Conference	2020
29	Alotaibi, Al-Turaiki, and Alakeel [39]	Journal	2020
30	Salahdine, and Kaabouch [40]	Conference	2021
31	Ripa, Islam, and Arifuzzaman [41]	Conference	2021
32	Dutta [42]	Journal	2021
33	Mughaid et al. [43]	Journal	2021
34	Mridha et al. [44]	Conference	2021
35	Li, Zhang, and Wu [45]	Conference	2022
36	Butt et al. [8]	Journal	2022
37	Magdy and Mikhail [46]	Journal	2022
38	Dewis and Viana [10]	Journal	2022

5. Discussion

Many researchers are still investigating BEC phishing attacks to identify better and more effective ways to counteract this growing threat. This paper serves as an excellent place for such researchers to begin understanding this paradigm by reviewing prior research that may be relevant to their study questions. To demonstrate how the reviewed papers have addressed our research questions, a discussion of the retrieved/analysed publications is provided in this section.

RQ1: What is the most recent and peer-reviewed literature regarding BEC phishing attacks?

To answer this research question, the retrieved/analysed publications that are related to BEC phishing attacks will be discussed. Table 3 summarises the contributions of each publication.

Table 3. Summary of recent studies in the literature regarding BEC phishing attacks.

Citation	Summary of Contribution	Limitations
Chakraborty and Mondal [11]	This paper analyses three DT classification algorithms for BEC phishing mail filtration. Logistic Model Tree classifier (LMT) produces the highest accuracy of 90%.	The accuracy achieved by the three DT classification algorithms is still low, and the model needs to be evaluated against a real-life dataset.

Table 3. *Cont.*

Citation	Summary of Contribution	Limitations
Qasem, Shamsuddin, and Zain [12]	This paper proposes a new hybrid multi-objective learning algorithm including MPPSON, MEPGAN, and MEPDEN to achieve a compact RBFN model with good prediction accuracy and prominent structure simultaneously for the process of detecting BEC attacks.	The proposed algorithms still suffer from slow convergence and long training times. There is a need to develop a sophisticated solution to overcome it.
Dhanaraj and Karthikeyani [13]	This paper uses Bayesian filtering to verify the sender's ID. The paper employs basic methods to differentiate humans from robot senders. The paper also creates new filters to detect emails requesting payment. The paper also uses N-gram language models, which assume that a word's location in a sequence depends on the previous N-l words.	The accuracy achieved is still low. More investigation into filtering methods is required to improve the effectiveness and processing time of the proposed models.
Shams and Mercer [14]	This paper presents a unique BEC and spam categorisation algorithm based on email content language and readability. Although it only works for English emails, it may be useful for other languages.	There is a need for additional testing to evaluate the effectiveness of classifiers generated by stacking multiple algorithms.
Laorden et al. [15]	This paper presents a study on the effectiveness of anomaly detection applied to BEC and phishing filtering techniques. The study identifies that more than 85% of received emails are BEC/spam/phishing.	The threshold selection needs to be automated to improve filtering results.
Rathod and Pattewar [16]	This paper presents a Bayesian machine learning algorithm classification for accurately detecting BEC and phishing emails in HTML format that have been pre-processed to remove HTML tags, and stop words are applied. The Bayesian classifier could categorise real-world Gmail data with an accuracy of 96.46%.	Malicious URL detection needs to be incorporated to improve the effectiveness of the proposed content-based detection model.
Zhu, Dong, and Liu [17]	This study find that the number of neighbours, the distance measure, and the decision rule are the primary factors influencing categorisation performance. Several distance functions and other KNN parameters that were examined in this research are integrated into a support vector machine (SVM) and neural network, along with a dimension reduction and closest-neighbour index construction.	Feature selection, dimension, and class numbers need to be investigated further to improve classification effectiveness.
Daeef et al. [18]	In this paper, BEC and spare phishing are discussed as major threats to stealing user data. The paper analyses phishing email classifiers based on the email header and body.	A dynamic phishing dataset is needed to test the effectiveness of the proposed BEC phishing detection model.
Yasin and Abuhasan [19]	This paper presents an intelligent classification model for detecting phishing emails using knowledge discovery, data mining, and text processing techniques. The model was built using an intelligent pre-processing phase that extracts a set of features from the email's header, body, and term frequency.	The accuracy achieved by the proposed classification algorithm is still low, and the model needs to be evaluated against real-life datasets by considering the email's body and term frequency.
Zweighaft [20]	This paper presents the concept of BEC as a type of spear phishing in which fake or fraudulent emails are sent to employees of a specific business. The paper also presents an approach to securing access to content with multi-factor authentication and staff training.	The study provides some suggestions to detect BEC phishing attacks without evaluating the effectiveness of the suggested techniques.
Rawal et al. [21]	This paper classifies BEC and phishing emails using a SVM and a Random Forest (RF) classifier and achieves an accuracy of 99. 87% with these algorithms.	The dataset used does not reflect real-life scenarios. A new dataset of real-life and dynamic emails is required.

Table 3. *Cont.*

Citation	Summary of Contribution	Limitations
Zeng [22]	This paper provides a predictive analytical technique that learns legitimate from harmful emails to overcome BEC attacks using static analysis.	Additional discriminating features need to be added to the predictive model to improve the accuracy of the detection model.
Moradpoor, Clavie, and Buchanan [23]	This paper presents an Artificial Neural Network (ANN) model algorithm classification for accurately detecting BEC and phishing emails. The ANN model contains ten hidden layers, five input features, one output layer, and one output feature. Confusion matrix, receiver operating characteristic (ROC), network performance, and error histogram are used to record, portray, and analyse the data. The ANN model achieves an accuracy of 96.46%.	Email word vectors are not enough to produce an effective detection model. Word embedding methods are required to vectorise full documents, rather than email word vectors, to improve the effectiveness of the detection model.
Niu et al. [24]	This paper proposes a novel SVM with Cuckoo Search (CS) detection model. The proposed approach detects more phishing emails than SVM with default parameters.	The proposed model utilizes only a single ML algorithm, so more algorithms are needed to evaluate the effectiveness of the model.
Peng, Harris and Sawa [25]	This paper presents attackers who pose as social networks, banks, IT administrators, or e-commerce sites. These emails may entice consumers to download malware or input personal information on a dangerous website. This study uses semantic analysis to check each phrase in an attacker's text.	The dataset used does not reflect the need for text emails, not graphics. A new dataset of text emails is required.
Baykara and Gurel [26]	This paper builds an "Anti-Phishing Simulator" to identify BEC attacks using various ML techniques.	This method needs a real-life scenario to evaluate the effectiveness of the model.
Sahoo [27]	This paper uses data mining approaches to examine emails and avoid BEC phishing attacks.	The study provides some suggestions without evaluating their effectiveness.
Hiransha et al. [28]	This paper explains how to spot phishing emails including BEC attacks and avoid falling into their traps in a comprehensive manner.	The dataset used does not reflect real-life scenarios. A new real-life dataset is required.
Singh, Pamula, and Shekhar [29]	This paper evaluates the performance of Non-Linear SVM-based classifiers with two different kernel functions (Linear Kernel and Gaussian Kernel) over the SpamAssasin Public Corpus dataset.	The proposed model needs to be evaluated against more ML algorithms and different datasets.
El Aassal et al. [30]	This paper proposes a Multinomial Naive Bayes (MNB)-based ML algorithmic classification model for detecting BEC and phishing content in emails. The proposed MNB models can classify BEC and phishing emails with 96.8% accuracy.	The proposed model detects phishing only from the email content without considering the email header.
Nidhin et al. [31]	This paper proposes a supervised classifier for BEC phishing and legitimate emails. The paper classifies authentic and fraudulent emails using Naive Bayse (NB), Logistic Regression (LR), Decision Tree (DT), RF, Adaboost, and SVM.	A feature selection technique is not discussed as part of the proposed classifiers. In addition, the dataset used does not reflect real-life scenarios
George Fomunyam [32]	This paper identifies that ML algorithms are more effective than traditional mechanisms in detecting and categorising spam letters from internet fraudsters. This study presents new ways to combat cybercriminals' fraudulent BEC phishing attacks.	This study provides some suggestions to detect BEC phishing without evaluating its effectiveness.

Table 3. *Cont.*

Citation	Summary of Contribution	Limitations
Oña et al. [33]	This paper develops a new method for identifying BEC attacks and countering them. The paper provides a comprehensive discussion about how to integrate autonomous learning, feature selection, and ANNs using Scrum. This technique can identify and counteract an email server-based phishing attack.	The proposed methods have been not evaluated against either benchmark datasets or real-life data.
Maleki and Ghorbani [34]	This paper proposes a K-means-based ML algorithmic classification model for detecting BEC content in emails. The proposed model can classify BEC attacks with 92% accuracy.	Dynamic feature selection is not provided. In addition, the dataset used does not reflect real-life scenarios.
Yang et al. [35]	This paper provides a BEC detection model by analysing email headers, URLs, and scripts. A total of 500 authentic and 500 phishing emails were used in the experiments. The proposed method achieves 99% true positive, 9% false positive, and 91.7% precision.	The dataset used does not reflect real-life scenarios. A new dataset of real-life and dynamic emails is required.
Garces et al. [36]	The paper investigates phishing web attack anomalies and how integrating ML techniques with data analytics can be a very effective solution to detect BEC attacks faster.	A real-life dataset is needed to check the effectiveness of the model for taking proactive decisions to minimise the impact of an attack.
Rendall, Nisioti, and Mylonas [37]	In this paper, the researchers investigate the use of a multi-layered detection framework in which a potential phishing domain is classified multiple times by models using different feature sets.	The proposed framework lacks the use of a sophisticated data fusion process as part of JDL level 2 (situation refinement).
Alam et al. [38]	This paper provides a BEC phishing detection model using the DT and RF techniques.	More ML-based algorithms are needed to evaluate the effectiveness of their model.
Alotaibi et al. [39]	This paper presents a convolutional ANN for BEC email phishing detection. The approach can help enterprises protect against phishing email attacks.	A feature selection technique is not discussed as part of the proposed BEC phishing detection model.
Salahdine, El Mrabet, and Kaabouch [40]	This paper proposes utilising SVM, LR, and ANN algorithms for detecting BEC and phishing content in emails. The proposed models achieve an accuracy of 94.5%, 77.3%, and 92.9% in ANN, SVM and LR, respectively.	The proposed models detect phishing only from the email content without considering the email header.
Ripa, Islam, and Arifuzzaman [41]	This paper proposes utilising RF, SVM, KR, KNN, and DT algorithms for detecting BEC and phishing content in emails. The proposed models achieve an accuracy of 96.8%, 96.6%, 92.28%, 94.09%, and 96.47% in RF, SVM, LR, KNN and DT, respectively.	A dynamic and real-life phishing dataset is needed to test the effectiveness of the proposed BEC phishing detection models.
Dutta [42]	This paper proposes a recurrent ANN and short-term memory algorithm for detecting BEC and phishing content in emails. The proposed model achieves an accuracy of 94.8%.	The accuracy achieved by the proposed algorithm is still low, and a better accuracy is needed for the detection model.
Mughaid et al. [43]	This paper discusses ML methods and new technological solutions for mitigating BEC attacks. This study utilizes ML-based algorithms to classify emails as BEC/phishing or non-BEC/non-phishing.	The feature selection algorithm needs to be refined to keep up with attackers' evolving toolkits.
Mridha et al. [44]	This paper proposes RF and ANN-based algorithmic classification models for detecting BEC and phishing URLs accurately. The proposed RF and ANN models can classify BEC and phishing URL legitimacy labels with 99% accuracy.	The proposed model needs a GUI-based web browser extension framework to provide better precision for the detection model.

Table 3. *Cont.*

Citation	Summary of Contribution	Limitations
Li, Zhang, and Wu [45]	This paper proposes a BEC/phishing email detection method based on the persuasion principle.	A feature selection technique is not discussed as part of the proposed model.
Butt et al. [8]	This paper proposes utilising SVM, LSTM, RF, LR, ANN, and NB algorithms for detecting BEC and phishing content in emails. The proposed models achieve an accuracy of 99.6%, 98%, 94.5%, 93.9%, 95%, and 97% in SVM, LSTM, RF, LR, ANN and NB, respectively.	The proposed models detect phishing only from the email content without considering the email header.
Magdy, Abouelseoud and Mikhail [46]	This paper introduces a deep learning model to detect BEC attacks. The proposed classifier is designed with an eye on validation accuracy, achieving fast and competitive performance, and promoting its use in practical applications.	A mechanism for improving linguistic processing with content-based features is needed to improve the effectiveness of the detection model.
Dewis and Viana [10]	This paper proposes a BEC/phishing responder as a solution that uses a hybrid ML approach combining natural language processing and deep learning to detect phishing and BEC emails. It has achieved an average accuracy of 99% with the LSTM model for text-based datasets.	The dataset used does not reflect real-life scenarios. A new dataset of real-life and dynamic emails is required.

Table 3 provides a summary of the contributions of the retrieved publications that are related to BEC phishing attacks. Looking at the various reviewed studies illustrates that there are some similarities and differences among various researchers. Some researchers presented a comparative study of various supervised and unsupervised ML techniques to provide an effective BEC phishing detection model that provides the highest accuracy, precision, recall, and F-measure to detect phishing emails. For example, Butt et al. [8], Ripa, Islam, and Arifuzzaman [41], and Chakraborty and Mondal [11] created a comparative study using various ML algorithms, including DT, SVM, LSTM, RF, LR, ANN, NB, KR, and DT, to identify a ML algorithm that provides the highest accuracy on a specific dataset. Other researchers provided hybrid ML-based techniques that combine two or more algorithms with changes in variables to provide better accuracy for the BEC phishing detection model. For instance, Dewis and Viana [10] proposed a hybrid ML-based approach combining NLP and deep learning to detect BEC phishing emails. Their LSTM model has achieved an average accuracy of 99% for text-based datasets. In addition, Qasem, Shamsuddin, and Zain [12] proposed a new hybrid multi-objective learning algorithm combining MPPSON, MEP-GAN, and MEPDEN to achieve a compact RBFN model with good prediction accuracy and prominent structure while detecting BEC attacks.

Furthermore, some researchers focused more on the detection algorithm by investigating the best ML algorithm to implement their BEC phishing detection model, while other researchers focused more on the feature selection techniques to identify the best features that ensure the creation of a high-accuracy BEC phishing detection model. For example, Rendall, Nisioti, and Mylonas [37] used a multi-layered detection system where a potential phishing domain is classified multiple times by models using different feature sets, while the studies by Salahdine, El Mrabet, and Kaabouch [40] and Ripa, Islam, and Arifuzzaman [41] focused more on identifying the best ML algorithm for the detection model by comparing their effectiveness against various datasets.

Evaluating the proposed BEC phishing detection models by various researchers also revealed another difference among the retrieved publications: some researchers utilised publicly available datasets, while other researchers utilised real-world and dynamic datasets that they created in specific circumstances to evaluate the effectiveness of their detection models. For example, Garces and Cazres [36], Ripa et al. [41], Alam et al. [38], Dewis and Viana [10], Mridha et al. [44], and Nidhin et al. [31] evaluated the effectiveness of their phishing detection model using Kaggle dataset, one of the most common datasets in phishing detection domain, while other researchers created their own datasets, such as Baykara and Gurel [26], Rawal et al. [21], etc.

RQ2: What are the common ML algorithms for developing ML-based BEC detection models?

The technique used to identify a BEC attack is important to the process of identifying such an attack. It is possible to utilise a wide variety of algorithms to guarantee accuracy, although their detection effectiveness differs. This section lists various techniques that have been used by various researchers to build a BEC phishing detection model, as shown in Table 4. The most common techniques include the following:

- **Naive Bayes (NB):** This classifier uses the Bayes theorem to classify data samples. The Bayes theorem asserts that, given a hypothesis H and some evidence E, the probability of each category is computed, and then the highest probability category is the output [47,48].
- **Support Vector Machines (SVM):** This classifier is a speedy and efficient supervised approach for text classification algorithms. The input training set generates a hyperplane, a two-dimensional line that best separates categories. This hyperplane is the decision boundary. In BEC detection, the input is a set of criteria, such as the presence or absence of specified words; the output, 1 or -1, indicates whether the email is a BEC attack. For instance, certain phrases can be used to detect whether an email is a BEC attack [48,49].
- **Logistic Regression (LR):** A binary logistic model uses one or more predictor variables to estimate the probability of a binary response (features). It allows stating that a risk factor boosts the possibility of a specific consequence by a certain percentage [47].
- **Decision Tree (DT):** This technique utilises a tree-like model of actions and their effects, including chance event outcomes, resource costs, and utility. It is one approach to present a conditional-only algorithm. DT is used in operation research, especially decision analysis, to discover the most probable method to attain a goal. It is also a popular machine learning technique [50].
- **Random Forest (RF):** This technique blends many DT outputs to obtain a single outcome. Its simplicity of use and versatility have spurred its popularity as a classification and regression tool [51].
- **Artificial Neural Network (ANN):** This technique is a collection of algorithms that attempt to replicate the way the human brain works to discover hidden patterns and connections within a dataset. Neuronal systems, whether biological or synthetic, are what we mean when we talk about neural networks [8].
- **Natural Language Processing (NLP)**: This is a subfield of computer science and, more specifically, a subfield of artificial intelligence (AI) that focuses on providing computers with the capacity to comprehend written and spoken language [52].

From Table 5, we can see that DT, SVM, ANN, NB, and Logistic algorithms have all been utilised in at least 10 of the 38 studies, indicating that researchers have found their results to be consistent enough to justify reusing these algorithms. In addition, it is important to highlight that certain algorithms, such as DT, SVM, NB, ANN, and Logistic algorithms, have a broad user base and are widely utilised by researchers and data scientists. As a result, they have well-updated libraries, and further enhancements are available to make them more compatible with several datasets due to their continuous use [53,54].

Table 4. List of algorithms used in the literature and their abbreviations.

Algorithm	Abbreviation
Linear Regression	Linear
Logistic Regression	Logistic
Decision Tree	DT
Support Vector Machine	SVM
Naive Bayes	NB
K-Nearest Neighbours algorithm	KNN
Random Forest	RF
Dimensionality Reduction Algorithm	DRA
Artificial Neural Network	ANN
Voted Perceptron	VP
Natural Language Processing	NLP
XGBoost Classifier	XGB
Group Method of Data Handling	GMDH
Probabilistic Neural Network	PNN
Genetic Programming	GP
Multilayer Perceptron	MP
Principal Component Analysis	PCA
Gaussian Kernel	GK

These algorithms have been used extensively by various researchers due to their effectiveness and accuracy in detecting BEC phishing attacks with various networks and datasets. Identifying the effective algorithm within each communication network should be the right course of action for an effective and successful BEC detection model. In addition, creating a hybrid technique that integrates two or more of these algorithms can yield an effective technique that can provide a better BEC phishing detection model.

In addition, if we look at supervised and unsupervised ML algorithms that have been utilised by researchers to build BEC phishing detection models, we find that most researchers prefer using supervised ML algorithms. For example, supervised ML algorithms, including DT, SVM, NB, and Logistic algorithms, were used in at least 10 of the 38 reviewed articles, while unsupervised algorithms, such as PCA, were utilised in only two of the 38 reviewed articles. Researchers prefer utilising supervised ML algorithms in BEC phishing detection models since unsupervised learning typically uses clustering algorithms to group email categories, such as BEC emails. However, a clustering algorithm would typically categorise many common categories (e.g., social emails and marketing emails), but since BEC emails are so rare, it results in low precision and many false positives. Therefore, supervised learning algorithms are more suitable for detecting BEC attacks at high precision.

It is also important to note that certain algorithms, such as GMDH, PNN, GP, MP, PCA, and GK, were used less than other algorithms; these algorithms were used in only one or two articles out of the 38 selected articles, making them less well known than the first group of algorithms. These algorithms may still not be known for various researchers to try and identify their effectiveness in various communication networks, but these algorithms can be the basis for creating an effective hybrid BEC phishing detection model in the near future.

Table 5. ML algorithms utilised by various researchers to build BEC phishing detection models.

Citation	SVM	RF	NLP	NB	ANN	DT	Linear	Logistic	VP	XGB	DRA	PNN	GP	MP	PCA	GK	KNN	GMDH
Fomunyam [32]	-	-	-	✓	✓	✓	-	-	-	-	-	-	-	-	-	-	-	-
Peng and Sawa [25]	-	-	✓	✓	-	-	-	-	-	-	-	-	-	✓	-	-	-	-
Baykara and Gurel [26]	-	-	-	✓	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Sahoo [27]	-	-	-	✓	-	-	-	-	-	-	✓	-	-	-	-	-	-	-
Garces and Cazres [36]	-	-	-	-	✓	-	-	✓	-	-	-	-	-	-	-	-	-	-
Oña et al. [33]	-	-	-	-	✓	-	-	-	-	-	-	-	-	-	-	-	-	-
Li and Wu [45]	-	-	-	✓	-	✓	-	-	-	-	-	-	-	-	-	-	-	✓
Salahdine et al. [40]	✓	-	-	-	✓	-	✓	✓	-	-	-	-	-	-	-	-	-	-
Rathod et al. [16]	-	-	-	✓	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Rawal et al. [21]	✓	✓	-	✓	-	-	-	✓	✓	-	-	-	-	-	-	-	-	-
Zeng [22]	✓	✓	-	✓	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Ripa et al. [41]	-	✓	-	-	-	-	-	✓	-	✓	✓	-	-	-	-	-	✓	-
Hiransha et al. [28]	✓	-	✓	-	-	-	-	✓	-	-	-	✓	✓	-	-	-	-	-
Butt et al. [8]	✓	-	-	✓	-	-	-	✓	-	-	-	-	-	-	-	-	-	-
Rendall et al. [37]	✓	-	-	✓	-	✓	-	-	-	-	-	-	-	✓	-	-	-	-
Alam et al. [38]		✓	-	-	-	✓	-	-	-	-	-	-	-	-	✓	-	-	-
Singh et al. [29]	✓	-	-	-	-	-	✓	-	-	-	-	-	-	-	-	✓	✓	-
El Aassal et al. [30]	-	-	-	✓	-	-	-	✓	-	-	-	-	-	-	-	-	-	-
Moradpoor et al. [23]	-	-	✓	-	✓	-	-	-	✓	-	-	-	-	-	-	-	-	-
Dutta [42]	-	-	-	-	✓	-	-	-	-	-	-	-	-	-	-	-	-	-
Yasin et al. [19]	✓	✓	✓	✓	-	-	-	-	-	✓	-	-	-	-	-	-	-	-
Mughaid et al. [43]	✓	-	-	-	✓	✓	-	✓	-	-	-	-	-	-	-	-	-	-
Magdy et al. [46]	-	-	-	-	-	✓	-	-	-	-	-	-	-	-	-	-	-	-
Dhanaraj et al. [13]	-	-	-	✓	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Chakraborty et al. [11]	-	-	-	✓	-	✓	-	✓	-	-	-	-	-	-	-	-	-	-
Zhu and Liu [17]	-	-	-	-	-	✓	-	-	-	-	-	-	-	-	-	-	✓	-
Qasem et al. [12]	-	-	-	-	✓	-	-	-	-	-	-	-	-	-	-	-	-	-
Shams et al. [14]	✓	-	-	✓	-	-	-	-	-	-	-	-	-	-	-	-	-	✓
Maleki et al. [34]	-	-	✓	-	-	-	✓	-	-	-	-	-	-	-	-	-	-	-
Dewis and Viana [10]	-	-	✓	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Mridha et al. [44]	-	✓	-	-	✓	-	-	-	-	-	-	-	-	-	-	-	-	-
Daeef et al. [18]	-	✓	-	-	-	✓	-	-	-	-	-	-	-	-	-	-	✓	-
Nidhin et al. [31]	✓	✓	-	✓	-	✓	-	✓	-	-	-	-	-	-	-	-	-	-
Yang et al. [35]	✓	-	-	-	-	-	-	-	✓	-	✓	-	-	-	✓	-	-	-
Alotaibi et al. [39]	-	-	-	-	✓	-	-	-	-	✓	-	-	-	-	-	-	-	-
Niu et al. [24]	✓	-	-	-	✓	-	✓	-	-	-	-	-	-	-	-	-	-	-

RQ3: What are the common datasets used in creating BEC detection models?

Building a ML-based technique requires having a dataset for training and testing the suggested model to identify its effectiveness and accuracy. There are many common datasets that have been used by various researchers to build BEC phishing detection models. Table 6 summarises the datasets used by various researchers to build BEC phishing detection models. This paper highlights the fact that many datasets were created previously and get regular updates from their creators. For example, the Nazario dataset gets regular updates with fresh sample data, with the latest being in 2021. Other examples are the Spam email dataset, which was compiled in 2010, the Phishing corpus in 2005, the Enron spam in 2006, and the Spamassassin dataset in 2002, all of which get regular updates. The titles of the datasets used by the 38 publications are further categorised in Table 6.

In addition, out of the 38 studies, more than half used customised datasets in their study. In light of the ever-shifting nature of BEC attacks, most of the researchers acquired email samples from actively running servers and organisations' email systems. To keep up with the latest trends and conduct an in-depth study of emerging BEC attack routes and methodologies, a dynamic and continuously updated dataset that captures a wide range of emails is required. This further supports the argument that new customised datasets from working contexts are more widely utilised in research than the standard datasets provided.

RQ4: What are the conventional features used in developing an effective BEC detection model?

There are three primary locations from which features used to detect BEC phishing attacks are often extracted: header, body, and URLs. The URL is a subset of both the header and the body; thus, it is not surprising that it is a frequently utilised detection feature.

- **Header Features:** The header of an email is the section of the message that includes the sender's and the recipient's email addresses, as well as the message's topic. The technical details necessary for prompt email delivery are included in each message's unique header. Internet header refers to the part of an email that contains the sender's and the recipient's email addresses, the topics, and the dates. An email's header also contains useful technical information including the sender's email address, the receiver's email address, and a unique Message ID.
- **Body Features:** The body of an email is the key section of the message. Most features for detection are crafted based on the text or are conceptually comparable to a defined dictionary word search or a set bag of words.
- **URL Features:** These are features derived from the links in the body of an email and the authorised sender domain, which are extracted to be analysed based on criteria and defined structure and would serve as a good indicator for detecting BEC attacks. Table 7 shows the features used by various researchers to build effective BEC detection models.

Table 6. Datasets utilised by various researchers to build BEC phishing detection models.

Citation	Spam Archive Corpus [39]	Nazario [45]	Enron Corpus. [34]	Kaggle [41]	Spam Assasine [45]	Spam Enron [46]	Avocado Corpus [28]	Phishing Corpus [46]	Custom
Fomunyam [32]	✓	-	-	-	-	-	-	-	-
Peng and Sawa [25]	-	✓	✓	-	-	-	-	-	-
Baykara and Gurel [26]	-	-	-	-	-	-	-	-	✓
Sahoo [27]	-	-	-	-	-	-	-	-	✓
Garces and Cazres [36]	-	-	-	✓	-	-	-	-	-
Oña et al. [33]	-	-	-	-	-	-	-	-	✓
Li and Wu [45]	-	✓	-	-	✓	-	-	-	-
Salahdine et al. [40]	-	-	-	-	-	-	-	-	✓
Rathod et al. [16]	-	-	-	-	-	-	✓	-	-
Rawal et al. [21]	-	-	-	-	-	-	-	-	✓
Zeng [22]	-	-	-	-	-	-	-	-	✓
Ripa et al. [41]	-	-	-	✓	-	-	-	-	-
Hiransha et al. [28]	-	-	-	-	-	-	✓	-	-
Butt et al. [8]	-	-	-	-	-	-	-	-	✓
Rendall et al. [37]	-	-	-	-	-	-	-	-	✓
Alam et al. [38]	-	-	-	✓	-	-	-	-	-
Singh et al. [29]	-	-	-	-	✓	-	-	-	-
El Aassal et al. [30]	-	✓	-	-	-	-	-	-	-
Yasin et al. [19]	-	-	-	-	-	-	✓	-	-
Mughaid et al. [43]	-	-	-	-	-	-	-	-	✓
Magdy et al. [46]	-	-	-	-	-	✓	-	✓	-
Dhanaraj et al. [13]	-	-	-	-	-	-	-	-	✓
Chakraborty et al. [11]	-	-	-	-	-	-	-	-	✓
Zhu and Liu [17]	-	-	-	-	-	-	-	-	✓
Qasem et al. [12]	-	-	-	-	-	-	-	-	✓
Shams et al. [14]	-	-	-	-	✓	✓	-	-	-
Laorden et al. [15]	-	-	-	-	✓	-	-	-	-
Maleki et al. [34]	-	-	✓	-	-	-	-	-	-
Dewis and Viana [10]	-	-	-	✓	-	-	-	-	-
Mridha et al. [44]	-	-	-	✓	-	-	-	-	-
Daeef et al. [18]	-	-	-	-	-	-	-	-	✓
Nidhin et al. [31]	-	-	-	✓	-	-	-	-	-
Yang et al. [35]	-	-	-	-	-	-	-	-	✓
Alotaibi et al. [39]	✓	-	-	-	-	-	-	✓	-
Niu et al. [24]	-	-	-	-	-	-	-	-	✓

Table 7. Common features used by various researchers to build BEC detection models.

Citation	Header	Body	URL
George Fomunyam [32]	✓	✓	-
Peng, Harris and Sawa [25]	✓	✓	-
Baykara and Gurel [26]	✓	✓	✓
Sahoo [27]	✓	✓	✓
Garces, Cazares, and Andrade [36]	-	✓	✓
Oña et al. [33]	✓	✓	-
Li, Zhang, and Wu [45]	✓	-	✓
Salahdine, El Mrabet, and Kaabouch [40]	✓	-	✓
Rathod and Pattewar [16]	✓	✓	-
Rawal et al. [21]	-	✓	✓
Zeng [22]	✓	✓	-
Ripa, Islam, and Arifuzzaman [41]	-	-	✓
Hiransha, Unnithan, and Kp [28]	✓	-	✓
Butt et al. [8]	✓	✓	-
Rendall, Nisioti, and Mylonas [37]	✓	-	✓
Alam et al. [38]	✓	-	✓
Singh, Pamula, and Shekhar [29]	-	✓	-
El Aassal et al. [30]	-	✓	-
Moradpoor, Clavie, and Buchanan [23]	-	✓	✓
Dutta [42]	-	✓	✓
Yasin and Abuhasan [19]	-	✓	✓
Mughaid et al. [43]	-	✓	-
Magdy, Abouelseoud, and Mikhail [46]	-	✓	-
Dhanaraj and Karthikeyani [13]	✓	-	-
Chakraborty and Mondal [11]	✓	✓	-
Zhu, Dong, and Liu [17]	-	✓	-
Qasem, Shamsuddin, and Zain [12]	-	✓	-
Shams and Mercer [14]	-	✓	-
Laorden et al. [15]	-	✓	-
Maleki and Ghorbani [34]	✓	✓	✓
Dewis and Viana [10]	-	✓	✓
Mridha et al. [44]	✓	✓	-
Daeef et al. [18]	✓	✓	-
Nidhin et al. [31]	✓	-	-
Yang et al. [35]	✓	-	-
Alotaibi, Al-Turaiki, and Alakeel [39]	✓	✓	-
Niu et al. [24]	✓	✓	✓

From Table 7, there is a large number of researchers utilising the body and header features, with a total of 28 researchers utilising the body and a total of 23 researchers utilising the header feature for BEC phishing detection. Furthermore, a total of 14 researchers used a combination of header and body features.

Moreover, the body feature is utilised by various researchers, as BEC is mainly focused on crafting a good email body to deceive corporations and their employees in which the content used in the BEC attacks includes a good and official mode or tone of writing to achieve the required level of deception. In addition, the header provides a good source for determining the authenticity of emails as most of the information, such as the sender's email address, SCL, and other vital components, which can serve as a good indicator for a malicious BEC email, will also be easily spotted from the header.

6. Challenges and Future Directions

BEC phishing attacks are particularly dangerous because they do not contain malicious links or dangerous email attachments. They are used to impersonate or compromise corporate or publicly accessible email accounts of executives or high-level employees, who are involved in finance or who wire transfer payments, to conduct fraudulent transfers, costing billions of dollars in damages. Detecting BEC phishing attacks is getting harder since hackers change their tactics regularly to deceive email recipients and BEC detection tools. There are several open issues and future research directions that still need to be investigated to provide an effective BEC phishing detection model, including the following:

- **Dynamic Feature Selection:** Feature selection is a practical way for data visualisation and a technique to increase the classification accuracy of classifiers. Feature selection aims to find the smallest subset of features with the highest amount of information. Applying dynamic feature selection for BEC phishing detection is significant to enable the detection model to determine the appropriate set of features from the list of features extracted for a specific situation in an automatic manner in order to build an effective BEC phishing detection system. This creates an adaptive feature selection method that dynamically selects features for prediction at any given time [55,56]. In some cases, some essential features that have high weights when computing similarity distances may not be beneficial to the detection outcome due to changes in users' behaviour and attack scenarios. Hence, allowing the phishing detection system to select appropriate features dynamically will provide the missing piece to allow the creation of adaptive and effective BEC phishing detection models [57]. Adopting dynamic feature selection can solve many issues of current BEC detection models and provide higher accuracy in BEC phishing detection.
- **Dataset Availability:** Datasets are designed to be used as a benchmark for ML-based phishing detection systems. The availability and dependability of datasets is another obstacle in utilising ML algorithms to build BEC phishing detection models. The availability of datasets is crucial to the design and effectiveness of any ML detector/classifier. Before developing a model, one must guarantee that appropriate amounts of data are available [58]. In addition, ML algorithms are data-hungry in which the more data are available, the better efficiency and performance it produces. However, there are no available datasets that imitate real-life scenarios in the BEC phishing detection domain. Although there are some datasets, such as Kaggle, Nazario, and Phishing Corpus, these datasets are becoming nearly obsolete as they contain static features that are no longer used in advanced BEC phishing attacks. There is a need for creating large datasets that capture real-life scenarios of different systems, corporations, and networks to enable researchers to evaluate their novel ML-based BEC phishing models as well as to provide optimisation to existing techniques.
- **NLP and Deep Learning**: Deep learning is a subset of representation learning where the model can automatically find the representations and features required for the classification task from the raw data. Deep-learning algorithms can provide better accuracy in BEC phishing detection by training on larger datasets, while traditional ML algorithms tend to reach a performance plateau quite quickly. Deep-learning algorithms are more effective in data classification processes because they have several hidden layers. Since, in BEC phishing detection, email/URL pairs are intrinsically made up of text elements, it is natural to use NLP techniques. The successful integra-

tion of NLP with deep learning can develop better accuracy in BEC phishing detection models [59]. More studies are required to investigate the integration of NLP with deep learning that allows us to combine the best of both approaches to create a better BEC phishing detection system.

- **Explainable AI for BEC Phishing Detection:** One of the major issues of most AI-based models is that they are acting as a black box, where the input and output data can be seen and observed but the processes and operations working in between cannot be seen. Explainable Artificial Intelligence (XAI) enables the conversion of black-box models to glass-box models by generating explanations. XAI-based models outperform experts, and these models are more dependable and trustworthy. The goals of XAI systems are not only to improve a task's competence and accuracy but also to provide explanations for how a specific decision is made [60]. Integrating ML with XAI can provide more effective BEC phishing detection models where XAI can be used for global and local interpretation to empower the AI-based system with trust and reliability. Hence, more studies are required to investigate the development of ML with XAI tools that can provide effective BEC phishing detection models that can outperform existing models.
- **Real-Time BEC Phishing Detection:** One of the necessities in every corporation is having the ability to provide real-time BEC phishing detection. Before disclosing a user's personal information on a phishing website, the prediction of a phishing detection approach must be provided. The fraudulent email must be blocked by a trustworthy phishing detection tool without disclosing the user's credentials to the hackers [61]. There is a need for more studies to develop a technique that can be easily used by everyone to detect non-legitimate and BEC phishing emails accurately in real time.

7. Conclusions

Research efforts have mostly focused on finding ways to stop basic phishing emails that use text as their medium. In recent years, attacks have come up with new and creative tactics to utilise BEC phishing emails to attack organisations and businesses. BEC phishing email is a legitimate-looking email meant to trick the receiver. These emails may download harmful software if the receiver clicks on dangerous links in the body. Tricking a user involves telling them their business email user information have changed and asking them to check in to evaluate the changes. Once users click on an obfuscated link, they are led to a rogue site, which steals their information and redirects them to the corporate site. Although there are some efforts made to create effective methods to detect BEC phishing emails, there is still a need for more work to investigate this topic further and to provide better and more effective solutions. This paper presents a systematic literature review and analysis of the state of the art of BEC phishing attacks. This paper systematically analyses journal articles and conference proceedings published between 2012 and 2022. Based on the selected search strategy, 38 articles (out of 950 articles) were chosen for a closer examination in terms of recent BEC phishing detection models, ML-based algorithms used to build these models, common datasets used to develop these models, and common features utilised to detect BEC phishing emails. The results provide a summarised version of selected articles to give readers a basic view of the state of the art of BEC phishing attacks. The results indicate that several researchers are interested in utilising ML-based techniques for detecting BEC attacks, as the number of BEC attacks is increasing daily and the attacks' measures are changing and evolving daily, with DT, SVM, ANN, NB, and Logistic algorithms being the most common techniques used by various researchers. In addition, there is a large number of researchers who have utilised the body and header features to detect BEC phishing attacks, with 28 articles utilising the body features, 23 articles utilising the header features, and 14 articles using a combination of both header and body features. The paper also presents challenges and future research directions related to BEC phishing detection based on ML. There is a need for more research studies on dynamic feature selection, creating real-life datasets, integrating NLP with deep learning, and combining ML with XAI to develop an effective and optimised BEC phishing detection system.

Author Contributions: Conceptualization, H.F.A. and O.O.; methodology, H.F.A.; Implementation, H.F.A. and O.O.; validation, H.F.A.; investigation, H.F.A. and O.O.; resources, O.O.; writing—original draft preparation, H.F.A. and O.O.; writing—review and editing, H.F.A.; visualization, H.F.A. and O.O.; supervision, H.F.A.; project administration, H.F.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Cidon, A.; Korshun, N.; Schweighauser, M.; Tsitkin, A.; Gavish, L.; Bleier, I. High Precision Detection of Business Email Compromise High Precision Detection of Business Email Compromise. In Proceedings of the 28th USENIX Security Symposium (USENIX Security 19), California, USA, 14–16 August 2019; Available online: https://www.usenix.org/system/files/sec19-cidon.pdf (accessed on 17 August 2020).
2. Cross, C.; Gillett, R. Exploiting trust for financial gain: An overview of business email compromise (BEC) fraud. *J. Financ. Crime* **2020**, *27*, 871–884. [CrossRef]
3. Jang-Jaccard, J.; Nepal, S. A survey of emerging threats in cybersecurity. *J. Comput. Syst. Sci.* **2014**, *80*, 973–993. [CrossRef]
4. Nisha, T.N.; Bakari, D.; Shukla, C. Business E-mail Compromise—Techniques and Countermeasures. In Proceedings of the 2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), Greater Noida, India, 4–5 March 2021. [CrossRef]
5. 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 Innternational Conference on Software Quality, Reliability and Security Companion (QRS-C), Macau, China, 11–14 December 2020. [CrossRef]
6. Compsysplus. Business Email Compromise Attacks-Computer Systems Plus. Available online: https://www.compsysplus.com/2021/07/the-10-stages-of-a-business-email-compromise-attack/ (accessed on 17 November 2022).
7. Cornish, D.B.; Clarke, R.V. Opportunities, precipitators and criminal decisions: A reply to Wortley's critique of situational crime prevention. *Crime Prev. Stud.* **2003**, *16*, 41–96.
8. Butt, U.A.; Amin, R.; Aldabbas, H.; Mohan, S.; Alouffi, B.; Ahmadian, A. *Cloud-Based Email Phishing Attack Using Machine and Deep Learning Algorithm*; Springer: New York, NY, USA, 2022. [CrossRef]
9. Karim, A.; Azam, S.; Shanmugam, B.; Kannoorpatti, K.; Alazab, M. A comprehensive survey for intelligent spam email detection. *IEEE Access.* **2019**, *7*, 168261–168295. [CrossRef]
10. Dewis, M.; Viana, T. Phish Responder: A Hybrid Machine Learning Approach to Detect Phishing and Spam Emails. *Appl. Syst. Innov.* **2022**, *5*, 73. [CrossRef]
11. Chakraborty, S.; Mondal, B. Spam Mail Filtering Technique using Different Decision Tree Classifiers through Data Mining Approach-A Comparative Performance Analysis. *Int. J. Comput. Appl.* **2012**, *47*, 26–31. [CrossRef]
12. Qasem, S.N.; Shamsuddin, S.M.; Zain, A.M. Multi-objective hybrid evolutionary algorithms for radial basis function neural network design. *Knowl. Based Syst.* **2012**, *27*, 475–497. [CrossRef]
13. Dhanaraj, S.; Karthikeyani, V. A study on e-mail image spam filtering techniques. In Proceedings of the 2013 International Conference on Pattern Recognition, Informatics and Mobile Engineering, Salem, India, 21–22 February 2013. [CrossRef]
14. Shams, R.; Mercer, R.E. Classifying Spam Emails Using Text and Readability Features. In Proceedings of the 2013 IEEE 13th International Conference on Data Mining, Dallas, TX, USA, 7–10 December 2013. [CrossRef]
15. Laorden, C.; Ugarte-Pedrero, X.; Santos, I.; Sanz, B.; Nieves, J.; Bringas, P.G. Study on the effectiveness of anomaly detection for spam filtering. *Inf. Sci.* **2014**, *277*, 421–444. [CrossRef]
16. Rathod, S.B.; Pattewar, T.M. Content-based spam detection in email using Bayesian classifier. In Proceedings of the 2015 International Conference on Communications and Signal Processing (ICCSP), Melmaruvathur, India, 2–4 April 2015. [CrossRef]
17. Zhu, S.; Dong, W.; Liu, W. Hierarchical Reinforcement Learning Based on KNN Classification Algorithms. *Int. J. Hybrid Inf. Technol.* **2015**, *8*, 175–184. [CrossRef]
18. Daeef, A.; Ahmad, R.B.; Yacob, Y.; Yaakob, N.; Bin, M.N.; Warip, M. Phishing Email Classifiers Evaluation: Email Body and Header Approach. *J. Theor. Appl. Inf. Technol.* **2015**, *80*, 354–361.
19. Yasin, A.; Abuhasan, A. An Intelligent Classification Model for Phishing Email Detection. *Int. J. Netw. Secur. Its Appl.* **2016**, *8*, 55–72. [CrossRef]
20. Zweighaft, D. Business email compromise and executive impersonation: Are financial institutions exposed. *J. Invest. Compliance* **2017**, *18*, 1–7. [CrossRef]

21. Rawal, S.; Rawal, B.; Pilani, B.; Goa, I.; Shaheen; Malik, S. ISSN: 2249-0868 Foundation of Computer Science FCS. *Int. J. Appl. Inf. Syst. (IJAIS)* **2017**, *12*, 21–24.
22. Zeng, Y.G. Identifying email threats using predictive analysis. In Proceedings of the 2017 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), London, UK, 19–20 June 2017. [CrossRef]
23. Moradpoor, N.; Clavie, B.; Buchanan, B. Employing machine learning techniques for detection and classification of phishing emails. In Proceedings of the 2017 Computing Conference, London, UK, 18–20 July 2017. [CrossRef]
24. Niu, W.; Zhang, X.; Yang, G.; Ma, Z.; Zhuo, Z. Phishing Emails Detection Using CS-SVM. In Proceedings of the 2017 IEEE International Symposium on Parallel and Distributed Processing with Applications and 2017 IEEE International Conference on Ubiquitous Computing and Communications (ISPA/IUCC), Guangzhou, China, 12–15 December 2017. [CrossRef]
25. Peng, I.T.; Harris, I.; Sawa, Y. Detecting Phishing Attacks Using Natural Language Processing and Machine Learning. In Proceedings of the 2018 IEEE 12th International Conference on Semantic Computing (ICSC), Laguna Hills, CA, USA, 31 January 2018–2 February 2018. [CrossRef]
26. Baykara, M.; Gurel, Z.Z. Detection of phishing attacks. In Proceedings of the 2018 6th International Symposium on Digital Forensic and Security (ISDFS), Antalya, Turkey, 22–25 March 2018. [CrossRef]
27. Sahoo, P.K. Data mining a way to solve Phishing Attacks. In Proceedings of the 2018 International Conference on Current Trends towards Converging Technologies (ICCTCT), Coimbatore, India, 1–3 March 2018. [CrossRef]
28. Hiransha, M.; Unnithan, N.A.; Vinayakumar, R.; Soman, K.P. Deep Learning Based Phishing E-mail Detection. In Proceedings of the 1st Antiphishing Shared Pilot 4th ACM International Workshop on Security and Privacy Analytics (IWSPA). Arizona, USA, 21 March 2018.
29. Singh, M.; Pamula, R.; shekhar, S.k. Email Spam Classification by Support Vector Machine. In Proceedings of the 2018 International Conference on Computing, Power and Communication Technologies (GUCON), Greater Noida, India, 28–29 September 2018. [CrossRef]
30. Aassal, A.E.; Moraes, L.; Baki, S.; Das, A.; Verma, R. Anti-Phishing Pilot at ACM IWSPA 2018. In Proceedings of the 1st Antiophishing Shared Pilor 4th ACM International Workshop on Security and Privacy Analytics (IWSPA), Tempe, AZ, USA, 21 March 2018; Available online: http://www2.cs.uh.edu/~{}shahryar/files/IWSPA-AP.pdf (accessed on 26 October 2022).
31. Unnithan, N.A.; Harikrishnan, N.B.; Vinayakumar, R.; Soman, K.P. Detecting Phishing E-mail using Machine learning techniques. In Proceedings of the 1st AntiPhishing Shared Pilot at 4th ACM International Workshop on Security and Privacy Analytics (IWSPA 2018), Tempe, AZ, USA, 21 March 2018.
32. Fomunyam, D.K.G. Machine Learning and the Business of Cyber Security. *Int. J. Civil Eng. Technol. (IJCIET)* **2019**, *10*, 353–359.
33. Oña, D.; Zapata, L.; Fuertes, W.; Rodríguez, G.; Benavides, E.; Toulkeridis, T. Phishing Attacks: Detecting and Preventing Infected E-mails Using Machine Learning Methods. In Proceedings of the 2019 3rd Cyber Security in Networking Conference (CSNet), Quito, Ecuador, 23–25 October 2019. [CrossRef]
34. Maleki, N. A Behavioral Based Detection Approach for Business Email Compromises. Master's Thesis, University of New Brunswick, Fredericton, NB, Canada, 2019.
35. Yang, Y.; Qiao, C.; Kan, W.; Qiu, J. Phishing Email Detection Based on Hybrid Features. *IOP Conf. Ser. Earth Environ. Sci.* **2019**, *252*, 042051. [CrossRef]
36. Garces, I.O.; Cazares, M.F.; Andrade, R.O. Detection of phishing attacks with machine learning techniques in cognitive security architecture. In Proceedings of the 2019 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA, 5–7 December 2019. [CrossRef]
37. Rendall, K.; Nisioti, A.; Mylonas, A. Towards a Multi-Layered Phishing Detection. *Sensors* **2020**, *20*, 4540. [CrossRef] [PubMed]
38. Alam, M.N.; Sarma, D.; Lima, F.F.; Saha, I.; Ulfath, R.-E.; Hossain, S. Phishing Attacks Detection using Machine Learning Approach. In Proceedings of the 2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT), Tirunelveli, India, 20–22 August 2020. [CrossRef]
39. Alotaibi, R.; Al-Turaiki, I.; Alakeel, F. Mitigating Email Phishing Attacks using Convolutional Neural Networks. In Proceedings of the 2020 3rd International Conference on Computer Applications & Information Security (ICCAIS), Riyadh, Saudi Arabia, 19–21 March 2020. [CrossRef]
40. Salahdine, F.; El Mrabet, Z.; Kaabouch, N. Phishing Attacks Detection A Machine Learning-Based Approach. In Proceedings of the 021 IEEE 12th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York, NY, USA, 1–4 December 2021. [CrossRef]
41. Ripa, S.P.; Islam, F.; Arifuzzaman, M. The Emergence Threat of Phishing Attack and The Detection Techniques Using Machine Learning Models. In Proceedings of the 2021 International Conference on Automation, Control and Mechatronics for Industry 4.0 (ACMI), Rajshahi, Bangladesh, 8–9 July 2021. [CrossRef]
42. Dutta, A.K. Detecting phishing websites using machine learning technique. *PLoS ONE* **2021**, *16*, e0258361. [CrossRef]
43. Mughaid, A.; AlZu'bi, S.; Hnaif, A.; Taamneh, S.; Alnajjar, A.; Abu Elsoud, E. An intelligent cyber security phishing detection system using deep learning techniques. *Clust. Comput.* **2022**, *25*, 3819–3828. [CrossRef]
44. Mridha, K.; Hasan, J.; Saravanan, D.; Ghosh, A. Phishing URL Classification Analysis Using ANN Algorithm. In Proceedings of the 2021 IEEE 4th International Conference on Computing, Power and Communication Technologies (GUCON), Kuala Lumpur, Malaysia, 24–26 September 2021. [CrossRef]

45. Li, X.; Zhang, D.; Wu, B. Detection method of phishing email based on persuasion principle. In Proceedings of the 2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), Chongqing, China, 12–14 June 2020. [CrossRef]
46. Magdy, S.; Abouelseoud, Y.; Mikhail, M. Efficient spam and phishing emails filtering based on deep learning. *Comput. Netw.* **2022**, *206*, 108826. [CrossRef]
47. Bagui, S.; Nandi, D.; Bagui, S.; White, R.J. Classifying Phishing Email Using Machine Learning and Deep Learning. In Proceedings of the 2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), Oxford, UK, 3–4 June 2019. [CrossRef]
48. Mantas, C.J.; Castellano, J.G.; Moral-García, S.; Abellán, J. A comparison of random forest based algorithms: Random credal random forest versus oblique random forest. *Soft Comput.* **2018**, *23*, 10739–10754. [CrossRef]
49. Bagui, S.; Nandi, D.; Bagui, S.; White, R.J. Machine Learning and Deep Learning for Phishing Email Classification using One-Hot Encoding. *J. Comput. Sci.* **2021**, *17*, 610. Available online: https://www.academia.edu/75025334/Machine_Learning_and_Deep_Learning_for_Phishing_Email_Classification_using_One_Hot_Encoding (accessed on 30 August 2022). [CrossRef]
50. Posevkin, R.; Bessmertny, I. Translation of natural language queries to structured data sources. In Proceedings of the 2015 9th International Conference on Application of Information and Communication Technologies (AICT), Rostov on Don, Russia, 14–16 October 2015. [CrossRef]
51. Simpson, G.; Moore, T. Empirical Analysis of Losses from Business-Email Compromise. In Proceedings of the 2020 APWG Symposium on Electronic Crime Research (eCrime), Boston, MA, USA, 16–19 November 2020. [CrossRef]
52. Spamassassin, P.C.; Index of /old/publiccorpus. spamassassin.apache.org. Available online: https://spamassassin.apache.org/old/publiccorpus/ (accessed on 16 November 2022).
53. Dada, E.G.; Bassi, J.S.; Chiroma, H.; Abdulhamid, S.M.; Adetunmbi, A.O.; Ajibuwa, O.E. Machine learning for email spam filtering: Review, approaches and open research problems. *Heliyon* **2019**, *5*, e01802. [CrossRef] [PubMed]
54. Schäfer, C. Detection of compromised email accounts used for spamming in correlation with mail user agent access activities extracted from metadata. In Proceedings of the 2015 IEEE Symposium on Computational Intelligence for Security and Defense Applications (CISDA), Verona, NY, USA, 26–28 May 2015. [CrossRef]
55. Bountakas, P.; Xenakis, C. Helphed: Hybrid Ensemble Learning Phishing Email Detection. *J. Netw. Comput. Appl.* **2023**, *210*, 103545. [CrossRef]
56. Salloum, S.; Gaber, T.; Vadera, S.; Shaalan, K. A Systematic Literature Review on Phishing Email Detection Using Natural Language Processing Techniques. *IEEE Access* **2022**, *10*, 65703–65727. [CrossRef]
57. Al-Musib, N.S.; Al-Serhani, F.M.; Humayun, M.; Jhanjhi, N.Z. Business email compromise (BEC) attacks. Materials Today: Proceedings. *Mater. Today Proc.* **2021**. [CrossRef]
58. Ahmed, C.M.; MR, G.R.; Mathur, A.P. Challenges in Machine Learning based approaches for Real-Time Anomaly Detection in Industrial Control Systems. In Proceedings of the 6th ACM on Cyber-Physical System Security Workshop, Taipei, Taiwan, 6 October 2020. [CrossRef]
59. Catal, C.; Giray, G.; Tekinerdogan, B.; Kumar, S.; Shukla, S. Applications of deep learning for phishing detection: A systematic literature review. *Knowl. Inf. Syst.* **2022**, *64*, 1457–1500. [CrossRef]
60. Aslam, N.; Khan, I.U.; Mirza, S.; AlOwayed, A.; Anis, F.M.; Aljuaid, R.M.; Baageel, R. Interpretable Machine Learning Models for Malicious Domains Detection Using Explainable Artificial Intelligence (XAI). *Sustainability* **2022**, *14*, 7375. [CrossRef]
61. Aljofey, A.; Jiang, Q.; Rasool, A.; Chen, H.; Liu, W.; Qu, Q.; Wang, Y. An effective detection approach for phishing websites using URL and HTML features. *Sci. Rep.* **2022**, *12*, 8842. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.