EasyChair Preprint

№ XXX

Organizational Human Factors and Technology Controls Against Phishing: A Qualitative Literature Synthesis and Classification Framework

Trinh Khanh, Le Phuong and Pham Thong

January 13, 2026

Organizational Human Factors and Technology Controls Against Phishing: A Qualitative Literature Synthesis and Classification Framework

Le Huy Phuong[1][0009-0007-3348-2455], Trinh Xuan Khanh[2][0009-0007-0755-2835] and Pham Viet Thong[3][0009-*0005-6480-5080*]

School of Science, Engineering and Technology, RMIT University, HCM City, Vietnam

Abstract. Phishing attacks represent one of the most pervasive cybersecurity threats facing organizations globally, with over 88% of enterprises reporting spear-phishing incidents and 88% of data breaches originating from employee mistakes. Despite substantial investments in security infrastructure, organizations remain vulnerable to social engineering methods that exploit human, organizational, and technological vulnerabilities. This research conducts a qualitative literature synthesis of 32 academic articles to identify and classify the most prevalent anti-phishing measures in two critical domains: Organizational Human Factors Controls and Technology Controls. Through systematic literature selection, categorization frameworks, and occurrence-based analysis, this study establishes a comprehensive classification system defining twelve organizational measure classes and eight technology control classes. Results reveal that Security Awareness Training Programs (100% occurrence), Incident Response Procedures (90%), and Phishing Simulation Programs (80%) constitute the core organizational defense framework, while Content-Based Detection Systems (50%) and URL-Based Detection Systems (40%) dominate technology controls. The study provides evidence-based implementation guidance for each high-frequency measure, including structured training methodologies, incident response team establishment, and hybrid detection architectures combining deep learning with traditional approaches. These findings offer enterprises, particularly emerging organizations, a data-driven prioritization framework for establishing comprehensive anti-phishing defenses that address both human vulnerabilities and technological gaps in contemporary threat landscapes.

Keywords: Phishing prevention, Security awareness training, Enterprise security, Anti-phishing measures, Organizational, human factors, Technology controls, Phishing detection, Incident response, Cybersecurity training, Machine learning phishing detection.

Table of contents

1. Introduction

In contemporary business environments, digital information constitutes a critical asset for organizational operations and competitiveness. Despite substantial investments in security infrastructure encompassing hardware, software, and administrative frameworks, enterprises remain vulnerable to social engineering methods, particularly phishing attacks. Phishing represents one of the most pervasive cybersecurity threats facing organizations globally. Research published in Computer Fraud & Security documented that over 88% of organizations across verticals reported facing spear-phishing attacks in 2019, which resulted in 46% receiving ransomware demands and 25% of small and medium-sized businesses (SMBs) suffering phishing attacks [1]. Contemporary phishing campaigns increasingly exploit mobile platforms, with approximately 60% of enterprises experiencing mobile-based attacks through SMS (smishing) and voice calls (vishing) [1].

The complexity of combating phishing stems from its multi-dimensional nature, exploiting vulnerabilities across three interconnected domains: human factors, organizational aspects, and technological controls, collectively referred to as the "HOT" framework [2]. Research published in IEEE Conference Proceedings demonstrates that these three elements share the common characteristic of human involvement, making security gaps inevitable [2]. Phishing security controls and vulnerabilities can be classified according to these three main elements, with each functioning simultaneously as both a security control and a security vulnerability [2].

The human factor remains particularly critical, as evidenced by research from Stanford University Professor Jeff Hancock and Tessian, which revealed that 88% of data breaches originate from employee mistakes, with nearly 50% of employees acknowledging they had made errors at work that could have led to security issues [3]. The study identified distraction as a primary factor, with 45% of respondents citing it as the principal reason for falling victim to phishing scams [3]. Additionally, 57% of remote workers reported being more distracted when working from home, further exacerbating organizational vulnerability to phishing attacks [3].

Given the evolving sophistication of phishing attacks and the persistent vulnerabilities in organizational systems, this report examines established countermeasure frameworks that address Organizational Human Factors Control and Technology Control methodologies. By synthesizing research on these two dimensions, this analysis establishes a foundational framework for emerging enterprises seeking comprehensive protection against phishing threats.

2. Methodology

The main objective of this report is to develop a general framework highlighting approaches that enterprises should take in terms of Organizational Human Factors control and Technology Control, in order to establish a robust anti-phishing environment. Given the nature of this research being explanatory and concept-driven, a Qualitative Literature Synthesis is considered the primary methodology approach and was used as such in this academic paper.

2.1.Literature Selection

A total of 32 grey and academic research papers were reviewed and analyzed, with all team members engaged in the reviewing process. The following criteria were applied during the filtering and selection stage:

- The paper must be indexed or discoverable via Google Scholar.
- The paper must be found using keywords such as *"enterprise phishing," "anti-phishing strategies," "phishing prevention in organizations,"* or similar.
- The publication must be no older than 10 years.
- The paper must explicitly discuss anti-phishing practices, techniques, or strategies within enterprise or organizational environments.

Only papers satisfying all criteria were reserved for detailed analysis.

2.2 Categorization Framework

Literature screening was followed by categorization frameworking, in which three primary categories of anti-phishing approaches were defined for data extraction and classification: **Human Factors, Technology Controls, and Organizational Aspects**

Within each category, individual measures identified through reading selected literature were grouped into "classes, with each class representing anti-phishing measures of a similar nature. For example, "implementation of software A to filter emails" and "implementation of software B to filter feedback" are both classified as "implementation of filtering software. Having qualitative definitions of classes was considered to likely cause confusion among readers, and therefore, to ensure consistency in categorization, each class was defined using the following attributes:

- **Name**: a standardized label representing a group(class) of similar anti-phishing measures.
- **Inclusion Criteria**: specific characteristics that determine whether a given measure should be categorized under the class.
- **Exclusion Criteria**: characteristics that disqualify a measure from belonging to the class.
- **Inclusion Examples**: sample instances demonstrating measures that correctly fit the class.
- **Exclusion Examples**: sample instances demonstrating measures that do not fit the class.
- **Number of Occurrences**: a counter indicating how many times measures belonging to this class appear across the 32 papers

2.3 Data Synthesis and Selection of Key Measures

After the counting process of results for the data table of three main categories, along with their classes, the table was analyzed to select the top 3 most numerous measure classes of each main category, which were selected based on the number of occurrences, totaling up to 9 measure classes. They were then recommended to future businesses in the Result section, as their high frequency of implementation suggests that they were, and still are, effective enough as anti-phishing measures that the majority of corporations chose to apply them in their business environment. Further review and a deep dive into how the aforementioned 9 measure classes were implemented among businesses are then discussed in the Discussion section to elaborate on how businesses can implement them. A simple recommendation might not provide sufficient information on the method and steps of implementation. Through both the Recommendation and further Discussion of those 9 measure classes, future young businesses can know what to apply and how to apply them for anti-phishing purposes.

3. Result

3.1 Organizational Human Factors Control

Organizational Human Factors Control Anti-Phishing Measures

Articles	Measures
Evaluating organizational phishing awareness training on an enterprise scale [4]	Simulated phishing attacks; Security awareness training programs; Click-through rate (CTR) monitoring; Reporting rate tracking; Personalized vs general phishing emails testing; Training waves implementation; Employee detection capabilities assessment
A review of organization-oriented phishing research [5]	Security policy frameworks; COBIT best practices implementation; Adequate policies and procedures to dictate employee behavior; Teaching employees to use technological controls; User and entity behavior analytics; Incident response procedures; Phishing report clustering approach; Community-based suspicious communication sharing

Prevention of Phishing Attacks: A Three-Pillared Approach [6]	Policy and process control; Awareness training programs; Organizational culture development; Simulated phishing exercises; Behavior modification programs; Employee education initiatives
Mitigation strategies against the phishing attacks: A systematic literature review [7]	Anti-phishing guidelines for organizations; Organizational awareness programs; Human-centered mitigation strategies; Technology-centric solutions combined with human factors; Comprehensive cybersecurity strategy
Employees' Behavior in Phishing Attacks: What Individual, Organizational, and Technological Factors Matter? [8]	Continuous security training programs; Educational programs; Procedural countermeasures (information security policy guidelines and rules); Detective countermeasures; Protective countermeasures; Well-designed security policy implementation
Phishing in Organizations: Findings from a Large-Scale and Long-Term Study [9]	Simulated phishing email campaigns; Click rate measurement; Credential submission tracking; Macro enabling monitoring; Reporting button deployment to corporate email client; Crowd-sourced phishing detection; Employee demographic analysis for targeting
A Case Study of Phishing Incident Response in an Educational Organization [10]	Phishing reporting systems; Help desk procedures for handling reports; Centrally managed security policy; Employee reporting requirements; Reactive defense processes; ITIL framework implementation; Distributed cognitive incident response; Mail relay filtering; Firewall updates; Multiple team coordination
Detection and prevention of spear phishing attacks: A comprehensive survey [11]	User awareness training programs; Incident response planning; Email authentication protocols (SPF, DKIM, DMARC); Multi-factor authentication implementation; Documented incident response plans; Legal frameworks and institutional policies; Training on email threats
Understanding the Efficacy of Phishing Training in Practice [12]	Annual security awareness training (mandatory); Unscheduled phishing exercises; Embedded training delivery; Office 365 and Proofpoint platform integration; User failure rate monitoring; Training completion tracking; Temporal relationship analysis between training and performance
Phishing Attacks: A Recent Comprehensive Study and a New Anatomy [13]	Interactive educational games (Anti-Phishing Phil); User education and training programs; Basic knowledge provision about suspicious emails; Reporting mechanisms to IT staff; Organizational awareness campaigns; Small/medium enterprise training focus
KnowBe4 Phishing by Industry Benchmarking Report 2025 [14]	Security awareness training (SAT) programs; Phishing simulations across organization; Phish-prone Percentage (PPP) measurement; Continuous training delivery; Simulated phishing combined with training; Baseline assessment before training; 90-day and 12-month reassessment

Study Confirms Security Awareness Training Significantly Reduces Susceptibility [15]	Phishing simulation programs; Pre-testing phishing response rate measurement; Internet Security Awareness Training (ISAT) implementation; Multiple phishing testing over weeks; Company-wide formal training programs; Simulated phishing email attacks; Templates for ongoing testing
Phishing Guidance: Stopping the Attack Cycle at Phase One (CISA) [16]	User training on social engineering and phishing; Documented incident response plans; DMARC configuration for emails; Phishing incident reporting procedures; Internal mail and messaging monitoring; Regular user education programs; Protective DNS resolver services
Combating phishing: A holistic human approach [2]	HOT framework (Human, Organizational, Technological); Best practices implementation; Policy and procedure assurance; Employee behavior guidelines; Teaching technological control usage; Organizational aspect controls; Policy formulation and enforcement
Retail Organization Case Study - Phish Alert Button [17]	Phish Alert Button (PAB) deployment; User reporting mechanism; Training on PAB usage; Simulated phishing campaigns; Phish-prone Percentage tracking; Learning management system integration; Coordinated training delivery
SOC Phishing Playbook - A Comprehensive Guide [18]	Phishing incident management framework; Incident detection procedures; Incident response coordination; Communication protocols; Post-incident activities; Continuous improvement processes; Computer Security Incident Response Team (CSIRT) structure; Incident prioritization framework; Incident classification system
PhiGARo: Automatic Phishing Detection and Incident Response Framework [19]	Phishing incident response framework; Honeypot-based detection; Phishing incident investigation procedures; Security incident management; Response strategy development; Incident handling procedures
Information security policy development and implementation [20]	Information security policy formulation; Policy implementation processes; Organizational recognition of policy importance; Security policy frameworks; Policy enforcement mechanisms
Anti-Phishing Training System for Security Awareness [21]	Anti-phishing training systems; Security awareness education; E-learning platforms; Training outsourcing alternatives; Cost-effective training implementation; Privacy-preserving training architecture
Evaluating the Effective Anti-Phishing Awareness and Training in Organizations [22]	Electronic mail phishing awareness measurement; Security training evaluation; Awareness programs in governmental organizations; Awareness programs in private organizations; Training importance measurement; Survey-based awareness assessment

Measure Classification Framework

To ensure systematic categorization and eliminate ambiguity in classifying organizational anti-phishing measures, this study developed a comprehensive Measure Classification Framework (Appendix 1). This framework defines twelve distinct measure classes, each characterized by five critical attributes: (1) a standardized name representing the measure group, (2) inclusion criteria specifying characteristics that qualify a measure for the class, (3) exclusion criteria identifying disqualifying characteristics, (4) inclusion examples demonstrating measures that correctly fit the class, and (5) exclusion examples showing measures that do not belong to the class. For instance, the "Security Awareness Training Programs" class is defined by formal training programs, awareness-raising methodologies, and educational content delivery as inclusion criteria, while explicitly excluding technology-only solutions and purely technical defenses as exclusion criteria. Concrete inclusion examples include "Implementation of annual security awareness training" and "Simulated phishing exercises with embedded training," whereas exclusion examples encompass "Email filtering software installation" and "Firewall configuration." This rigorous classification approach was applied consistently across all 20 academic articles reviewed, enabling precise counting of measure occurrences. The framework revealed that Security Awareness Training Programs appeared in all 20 articles (100%), followed by Incident Response Procedures in 18 articles (90%), and Phishing Simulation Programs in 16 articles (80%). Conversely, measures such as Recruitment of Security-Skilled Personnel appeared in only 5 articles (25%), indicating lower adoption prevalence. Each measure class in Table of Appendix 1 includes the complete set of academic source citations where the measure was identified [2][4][5][6][7][8][10][11][12][13][14][15][16][17][18][19][20][21][22], providing full traceability to the original literature and enabling readers to verify the classification decisions. This classification framework serves as the methodological foundation for objectively identifying which organizational measures are most widely discussed across various enterprise contexts in academic literature.

Organizational Human Factors Controls Measure Occurrence Summary

Building upon the classification framework, Appendix 2 presents a ranked summary of all twelve organizational anti-phishing measures based on their occurrence frequency across the 20 academic articles analyzed. This summary table provides four key dimensions for each measure: (1) overall ranking from most to least prevalent, (2) absolute number of articles mentioning the measure, (3) percentage of total articles discussing the measure, and (4) primary source citations for verification. The ranking reveals a clear hierarchical pattern in organizational anti-phishing approaches documented in academic literature. Security Awareness Training Programs dominate with 100% coverage across all articles [2][4][5][6][7][8][11][12][13][14][15][16][21][22], establishing it as the most universally recognized organizational countermeasure. The top tier (measures appearing in ≥75% of articles) comprises Security Awareness Training Programs (100%), Incident Response Procedures (90%), Phishing Simulation Programs (80%), and Security Policy Implementation (75%), indicating these four measures form the core organizational defense framework against phishing threats as consistently emphasized across diverse academic studies. The middle tier (40-70% occurrence) includes Baseline Assessment and Metrics (70%), Phishing Reporting Mechanisms (60%), Employee Communication and Culture Building (50%), ITIL/Framework Adoption (45%), and Multi-Factor Authentication Policy (40%), representing supplementary yet significant organizational controls. The lower tier (≤35% occurrence) encompasses Regular Security Audits and Monitoring (35%), Email Authentication Protocol Implementation (30%), and Recruitment of Security-Skilled Personnel (25%), suggesting these measures receive less consistent emphasis in academic literature. This occurrence-based ranking provides enterprises with evidence-based prioritization guidance, suggesting that organizations should first establish the top-tier measures documented across the broadest range of academic research before implementing lower-frequency measures. The distribution reveals that while some measures enjoy near-universal recognition in academic discourse, others remain specialized approaches potentially applicable to specific organizational contexts or industry sectors.

3.2 Technology Controls

Technology Controls Anti-Phishing Measures

Articles	Measures
Phishing Website URL Detection Using a Hybrid Machine Learning Approach [25]	**URL-based phishing detection** using a **hybrid machine learning approach**; lexical and structural URL analysis; domain age verification; machine learning classification of phishing and legitimate URLs
Integrated machine learning model for URL phishing detection [26]	**URL-based phishing detection** using a multi-filter machine learning architecture; lexical URL feature extraction; domain age verification; URL structural analysis; heuristic scoring mechanisms for phishing classification
Double-Layer Detection of Internal Threat in Enterprise Systems Based on Deep Learning [27]	**Behaviour-based and content-based phishing detection** at the enterprise level; phishing email detection using an LSTM–XGBoost model; user behaviour log analysis; insider threat identification using Bi-LSTM with attention mechanisms applied to enterprise activity logs
CNN-based phishing attack detection model for e-business in enterprise information systems [28]	**URL-based phishing detection** using deep learning; automated URL classification with 1D Convolutional Neural Networks (Conv1D); automatic learning of URL feature representations; classification of phishing and legitimate websites in enterprise e-business platforms
LSTM Based Phishing Detection for Big Email Data [30]	**Content-based phishing email detection** using Natural Language Processing (NLP); email body text preprocessing; Word2Vec embedding generation; sequential content modelling using Long Short-Term Memory (LSTM) networks; automated email sample labelling using KNN and K-Means; large-scale enterprise email stream analysis
Intelligent phishing detection scheme using deep learning algorithms [31]	**Hybrid phishing detection** combining URL-based, content-based, and visual analysis; CNN for feature extraction and LSTM for sequence modelling; analysis of URL features, webpage text, HTML frame structures, and visual image characteristics; automated website classification

Detecting Credential Spearphishing Attacks in Enterprise Settings [32]	**Metadata- and behaviour-based credential phishing detection**; content-agnostic analysis using sender reputation and domain reputation scoring; correlation of SMTP, HTTP/NIDS, and LDAP user activity logs; unsupervised Directed Anomaly Scoring (DAS) for enterprise credential spear-phishing detection
Enterprise Credential Spear-phishing Attack Detection (ECSPAD) [33]	**Rule-based enterprise credential phishing detection**; look-alike and typosquatted domain detection; domain similarity scoring using SCP and NCC metrics; SPF and DKIM validation; domain and IP whitelisting; impersonation detection of trusted enterprise domains
Benchmarking and Evaluating Large Language Models in Phishing Detection for Small and Midsize Enterprises [34]	**Content-based phishing email detection using Large Language Models (LLMs)**; prompt-driven zero-shot inference; semantic and contextual analysis of phishing language patterns; likelihood scoring and explanation generation; benchmarking proprietary and open-source LLMs for cost–accuracy trade-offs

Table X: Technology-Based Anti-Phishing Detection Measures Identified in Enterprise-Focused Academic Studies

Measure Classification Framework

To ensure systematic and objective categorization of technology-based anti-phishing measures, this study developed a dedicated **Technology Controls Measure Classification Framework** (Appendix 3). This framework defines eight distinct measure classes, each characterized by five key attributes: (1) a standardized class name representing a group of technical solutions, (2) inclusion criteria specifying the technical characteristics required for membership in the class, (3) exclusion criteria identifying characteristics that disqualify a measure from the class, (4) inclusion examples illustrating representative technologies, and (5) exclusion examples demonstrating technologies that do not belong to the class.

For instance, the **Content-Based Detection Systems** class utilizes Natural Language Processing (NLP), deep learning, or Large Language Models (LLMs) to analyze email or web content for phishing characteristics. Inclusion criteria include textual feature extraction, semantic and contextual modelling, and content-based classification. Exclusion criteria explicitly omit URL-only analysis, metadata-only detection, and purely rule-based approaches. Representative inclusion examples comprise LSTM-based email classification [30], hybrid content detection with CNN+LSTM [31], and LLM-based phishing detection [34], whereas exclusion examples include URL reputation filtering and manual phishing awareness training.

Similarly, the **URL-Based Detection Systems** class includes automated analysis of URL lexical, structural, and statistical features to identify phishing sites, while explicitly excluding content-only detection, human feedback–dependent methods, and non-automated URL checks. Other classes include **Hybrid Multi-features System, Behaivour-based detection, Metadata-based detection**, **Rule-Based Detection**, and **LLM-Assisted Semantic Detection**, each defined with similar rigor using technical inclusion/exclusion criteria.

The framework was applied consistently across all ten technology-focused articles reviewed in Section 3.2.1, mapping each reported technological control to one or more measure classes based on its core detection functionality. This approach ensures methodological consistency, minimizes subjective interpretation, and enables accurate counting of occurrences across diverse machine learning, rule-based, and hybrid detection systems. Appendix 3 provides complete definitions, inclusion/exclusion criteria, and illustrative examples for transparency, reproducibility, and future comparative research.

Technology Controls Anti-Phishing Measure Occurrence Summary

Building upon the classification framework, Appendix 4 presents a ranked occurrence summary of all identified technology-based anti-phishing measures based on their frequency of appearance across the ten academic articles analyzed. Each measure class is reported with four dimensions: (1) overall ranking, (2) absolute number of articles mentioning the measure, (3) percentage of total technology-focused articles, and (4) primary source citations.

The analysis reveals that **Content-Based Detection Systems** are the most prevalent, appearing in **5 of 10 articles (50%)** [27][29][30][31][34], highlighting the adoption of NLP, LSTM, CNN, and LLM-based approaches in enterprise email and web content analysis. **URL-Based Detection Systems** follow closely, appearing in **4 articles (40%)** [25][26][28][31], reflecting their effectiveness in detecting malicious links and phishing websites.

Hybrid Multi-Feature Detection Frameworks, which integrate URL, content, HTML, and visual features, appear in **2 articles (20%)** [27][31], demonstrating the trend toward multi-dimensional detection for improved accuracy. **Behaviour- and Metadata-Based Detection Systems**, focusing on user behaviour logs, sender/domain reputation, and anomaly detection, are reported in **2 articles (20%)** [27][32], often associated with credential spear-phishing and insider threat mitigation.

Lower-frequency but notable classes include **Rule-Based Enterprise Detection Systems** (**1 article, 10%**) [33], such as domain similarity scoring, SPF/DKIM validation, and impersonation detection, and **LLM-Assisted Semantic Detection** (**1 article, 10%**) [34], reflecting its status as an emerging but promising approach. Real-Time Threat Monitoring and Automated Incident Response Integration were not directly represented in the reviewed dataset, indicating that continuous monitoring and automated workflow integration remain areas for future enterprise implementation.

This occurrence-based ranking provides evidence-based guidance for enterprises aiming to implement technology controls against phishing. Organizations are advised to prioritize content- and URL-based automated detection systems as foundational technical defenses, followed by hybrid, behaviour- and metadata-based approaches as their monitoring infrastructure and analytical maturity increase. Collectively, the classification framework and occurrence summary offer a structured, data-driven foundation for evaluating the relative prevalence, strategic importance, and emerging trends of technology-based anti-phishing controls in contemporary enterprise environments.

4. Discussion

This part of the report aims to discuss the currently universally accepted anti-phishing measures in categories of Organizational Human Factors Control and Technology Control. The reason for the implementation of the aforementioned anti-phishing measures will be discussed along with common methods of implementation

4.1 Organizational Human Factors Control

As can be referenced from the above result, ***Security Awareness Training*** is a priority among enterprises due to many reasons: Firstly, human involvement in organizational structure and interaction with technology is common if not inevitable, and therefore, resolving human behaviors is essential to address phishing threats satisfactorily [2]. Secondly, several researchers noted the benefits of well-designed security awareness training for reducing employees' click rates on phishing emails [4], [15]. Thirdly, Security Awareness Training can be considered a simple non-technical solution that can more easily be implemented by Corporations whether big or small [23] [24]. On further examination of Security Awareness training, it can be implemented through several ways:

- Phishing recognition and awareness training programs: Which are to introduce users to concepts of cybersecurity and identification of phishing emails through [2] [6]. Other exercise types can be considered, such as Embedded training delivery, Interactive educational games [12] [13]. In addition, the training program should be scheduled and done frequently enough so that employees retain security awareness during their time working for their respective company [35]. Regular refresher courses or tests ought to be handed out monthly to ensure security awareness retention [35].
- Technical training in various platforms, devices, software, and browsers: Which is to train employees to handle file types, web browsers, and system warning alerts, email clients, logging off/locking workstations, and anti-malware software that is currently present on the company's technical framework [2]. Employees being used to the company's devices and systems will likely make fewer accidental mistakes in handling real-life phishing scenarios.

Incident Response Procedures are also considered universal among solutions, taking up to 90% coverage out of 20 articles. Reasons for the implementation of a response procedure is mainly because preventative measures are not always fool-proof and provide guaranteed protection against Phishing as human errors can occur or gaps in security can be exposed [5] [10] . Due to the inevitability of successful phishing incidents, companies must always be prepared to detect, contain, and recover from breaches to minimize damage once the unavoidable happens.

To set an Incident Response Plan, an Incident response team should be established to handle specific responsibilities while not interfering with the company's operation. As such, a response team consisting of experts from various domains from either IT security, legal, human resources or public relations should be of consideration due to their versatility and employment of already present employees from essential departments of a company[11]. As the first line of defense in an Incident Response Plan, the response team should have access to tools that allow for the detection and analysis of incidents, which, more specifically, is to monitor unusual activity and help identify and analyze potential phishing attempts [11]. In case of a successful phishing attempt however, a containment and eradication process needs to be put in place and is handled by the response team in order to minimize the damage of such an incident, through essentials actions such as revoking unauthorized access, isolating impaired devices or eliminating malicious content [11]. Following a successful response, restoration of affected systems is to be enacted in order to ensure the continuation of business operations and availability of services [11]. Documentation or reporting of incidents is of importance post-attacks, and should be created through recording of the attack, the response and the recovery process in order to allow for review of the current security mechanism and subsequent improvement on either the response plan itself or any other technological, or human factor/organizational aspect[5] [11].

4.2 Technology Control

As shown in the results, **Content-Based Detection Systems** are the most widely adopted technology-based anti-phishing measures, appearing in **5 of 10 reviewed articles (50%)**. The primary reason for their widespread implementation is that phishing attacks increasingly exploit sophisticated social engineering techniques within emails and web content, which cannot be fully addressed through URL analysis alone. Content-based detection leverages Natural Language Processing

(NLP), semantic modelling, and machine learning approaches such as LSTM networks or Large Language Models (LLMs) to identify phishing indicators embedded in text, HTML, or other digital content [27][29][30][31][34].

The implementation of **Content-Based Detection** in enterprise contexts commonly includes automated **email content** parsing, feature extraction of keywords and phrases, contextual analysis, and semantic similarity scoring. For instance, LSTM-based models can process sequential patterns in email content to identify unusual or suspicious language structures, while LLMs enable zero-shot inference on previously unseen phishing campaigns, providing adaptive protection without requiring manual rule updates [34].

URL-Based Detection Systems, appearing in **4 articles (40%)**, are the second most prevalent measure. These systems focus on automated evaluation of URL characteristics, including lexical analysis, domain age verification, structural assessment, and heuristic or statistical scoring to detect potentially malicious links [25][26][28][31]. URL-based detection is widely implemented because phishing attacks often involve look-alike domains or obfuscated links designed to deceive users into divulging credentials. By automatically analyzing URLs and flagging high-risk links, these systems provide rapid, scalable protection that complements human awareness efforts. In practice, organizations can deploy URL filtering modules within email gateways, web proxies, or security appliances to prevent user access to known or suspicious phishing domains.

Hybrid Detection Frameworks, combining content and URL analysis with additional features such as visual inspection or HTML structure assessment, are reported in **2 articles (20%)** [27][31]. These systems aim to improve detection accuracy by integrating multiple input types, thereby addressing the limitations of single-modality approaches. For example, a hybrid model might analyze both the textual content of an email and the embedded URL patterns while also checking the visual similarity of a phishing webpage to legitimate sites. This multi-dimensional approach reduces false negatives and provides more comprehensive protection against increasingly sophisticated phishing campaigns.

In applying these solutions to our own organization, a multi-layered deployment strategy is recommended. For Content-Based Detection, enterprise email servers can integrate NLP or deep learning–based filters that automatically scan inbound messages for phishing indicators, leveraging pre-trained models or in-house fine-tuned classifiers. For URL-Based Detection, web gateways and email security tools should enforce automatic blocking or warning mechanisms for high-risk URLs, complemented by centralized logging for security monitoring. Hybrid Detection can be applied selectively for high-risk systems or sensitive departments, where email content, URLs, and web page snapshots are analyzed jointly to maximize detection reliability.

Together, these technology controls provide complementary layers of defense that reinforce human-factor measures, such as Security Awareness Training and Incident Response Procedures, creating a holistic anti-phishing strategy. By combining automated, data-driven detection with proactive human education, organizations can effectively reduce phishing success rates while maintaining scalable and sustainable security operations.

5. Conclusion

As technology evolves and rises, so will enterprise dependence on digital assets, and as such, sufficient protection needs to be provided to protect against attempts of unauthorized access to digital information. Implementing security for digital infrastructure are common practice by companies, but they are unable to effectively protect against social engineering schemes, more specifically, phishing still remains a problem that can bypass many layers of defense. However, there were, and still are, remedies for the threat of phishing, as many companies have implemented several organizational human factor

controls along with technological controls that can make employees and the enterprise's digital infrastructure less vulnerable. Through selective academic report filtering and the establishment of categorization tables, we were able to identify some of the most common anti-phishing measures belonging to 2 categories of **Organizational Human Factor Control**, and **Technology Control,** along with their reason to be implemented, and how such measures were implemented.

For **Organizational Human Factors,** Security Awareness Training programs, and Incident Response Plans were preferred by most, if not all, of the cases reviewed through Qualitative Literature Synthesis of 32 reports. The former solution is aimed at resolving the core cause of the phishing threat, which is the lack of awareness and recognition of the phishing threat by employees. The latter solution is considered by many to be both a necessity and a damage control method due to the inevitability of a phishing attack being successful. Security Awareness Training programs usually consist of multiple activities and exercises: simulated phishing exercises; Embedded training delivery, Interactive educational games, and can be implemented through the organization of aforementioned exercises. Implementation of Incident Response Plans is rather self-explanatory, and can be done through establishing a response team, having a phishing incident detection method, a recovery and protection scheme in case of a successful breach, and production of an audit for each incident for future review and assessment.

Technological controls complement human-centered defenses by providing automated mechanisms for the detection and prevention of phishing attacks. Many modern anti-phishing systems adopt **a modular or multi-stage architecture**, in which different analytical models process distinct data sources, and their outputs are subsequently aggregated to produce a final classification decision. **Content-based phishing detection systems** commonly employ deep learning models such as **LSTM networks**, often combined with a secondary decision-making or classification model to enhance accuracy. This architectural pattern is consistently observed across other technological measures, including **URL-based analysis, metadata inspection, and user behavior log analysis**. In these approaches, deep learning models are leveraged for feature extraction and pattern recognition, while complementary decision-making models integrate and evaluate the results to determine phishing likelihood. Furthermore, there is **a growing trend** toward **hybrid detection mechanisms**, in which enterprise systems simultaneously analyze multiple data types—such as email content, URLs, and behavioral signals—to achieve more robust and reliable phishing detection.[36]

Both anti-phishing categories of **Organizational Human Factors** and **Technology Control** are to be implemented in tandem to achieve optimal protection, and the measures presented above should either be self-explanatory enough for companies to implement, or referenced commonly enough so in vast amount of resource whether academic or commercial, that enterprises can easily consult on such resource and have a proper guide on how to implement them.

6. Appendix

Appendix 1: Measure Classification Framework

Measure class	**Definition**	**Inclusion Criteria**	**Exclusion Criteria**	**Inclusion Case**	**Exclusion Case**	**Number of Occurrences**
Security Awareness Training Programs	Active organizational commitment to training activities that raise awareness and enhance	-Description of formal training programs for employees -Awareness-raising	-Technology-only solutions without a human training	"Implementation of annual security awareness training" "Simulated	"Email filtering software installation" "Firewall configuration	[20] [2][4][5][6] [7][8][12][13][14][15][16][21][22]

	employee skillset against phishing threats through structured programs	methodologies -Workshop events -Effective human resource policies -Educational content delivery	component -Purely technical defenses -Automated systems without user education	phishing exercises with embedded training" "Interactive educational games for phishing recognition"	" "Antivirus deployment"	
Security Policy Implementation	Establishment and enforcement of formal documented policies, procedures, and guidelines that govern employee behavior and organizational security practices	-Written security policies -Procedural guidelines -Access control policies -Acceptable use policies -Security governance frameworks -Policy enforcement mechanisms	-Informal practices - Undocumented procedures -Technical controls without a policy framework -Individual actions not based on organizational policy	"Centrally managed security policy implementation" "COBIT framework adoption" "Information security policy guidelines and rules" "ITIL framework for service management"	"Ad-hoc security decisions" "Individual employee choices" "Unwritten practices"	[15][2][5][8][10][16][20]
Incident Response Procedures	Structured organizational processes and frameworks for detecting, reporting, analyzing, containing, and recovering from phishing attacks	-Documented response plans -Incident management workflows -Reporting mechanisms -Response team structures (CSIRT) -Post-incident analysis -Coordination protocols	-Purely reactive ad-hoc responses -Individual responses without an organizational framework -Technical detection without response procedures	"Phishing incident response framework implementation" "CSIRT team establishment " "Help desk procedures for phishing reports" "Incident prioritization and classification"	"Individual employee reporting to colleague" "Uncoordinated technical fixes" "One-time incident handling"	[18][5][9][10][11][16][18][19]
Phishing Simulation Programs	Organized campaigns sending simulated phishing emails to employees	-Simulated phishing email campaigns -Controlled testing	-Real phishing attacks -One-time	"Monthly simulated phishing campaigns"	"Actual phishing attack analysis"	[16][4][9][12][14][15][17]

	to test susceptibility and provide training opportunities	environment -Metrics collection (click rates, reporting rates) -Integration with training programs -Periodic testing schedules	tests without an organizational program -External penetration testing is not focused on phishing	"Phish-prone percentage measurement through simulations" "Embedded training after clicking simulation"	"Third-party penetration test" "Vulnerability scanning"	
Phishing Reporting Mechanisms	Tools, systems, and processes enabling employees to easily report suspected phishing attempts to security teams	-Reporting button/plugin (e.g., Phish Alert Button) -Dedicated reporting email addresses -Help desk hotlines -Ticketing systems for phishing reports -Reporting workflow integration	-General IT support without phishing-specific reporting -Informal communication channels -Technical detection systems without user reporting capability	"Phish Alert Button deployment in email client" "Dedicated phishing hotline" "Reporting button with one-click functionality"	"General help desk for all IT issues" "Email to supervisor" "Automated detection system only"	[12] [9][10][13][16][17][18]
Baseline Assessment and Metrics	Systematic measurement of organizational phishing vulnerability before interventions to establish a baseline and track improvement	-Pre-training vulnerability assessment -Phish-prone Percentage (PPP) calculation -Click-through rate (CTR) measurement -Initial risk assessment -Benchmark establishment	-Post-intervention measurement only -Informal observations -External threat assessments -General security audits not specific to phishing	"Baseline PPP measurement before training" "Initial phishing simulation to assess risk" "Pre-training phishing susceptibility testing"	"Annual security audit" "Compliance assessment" "Post-training evaluation only"	[14] [4][9][12][14][15][17]
Multi-Factor Authentication (MFA) Policy	Organizational mandate requiring additional authentication beyond passwords for accessing systems and data	-MFA implementation requirements -Phishing-resistant authentication methods -Authentication policy enforcement -Number	-Single-factor authentication -Optional MFA -Password-only policies -Technical MFA	"Mandatory MFA for all users" "Phishing-resistant MFA requirement for privileged accounts" "MFA policy with number	"MFA as an optional feature" "MFA available but not required." "Technical capability without policy"	[8] [11][16]

		matching implementation -Privileged user MFA requirements	deployment without policy	matching"		
Employee Communication and Culture Building	Organizational efforts to create a security-conscious culture through communication, leadership support, and community engagement	-Security culture development -Open communication about threats -Leadership support initiatives -Community-based threat sharing -Non-punitive reporting culture -Security awareness campaigns	-Training programs (covered separately) -Technical communications -Policy enforcement actions -Individual manager actions	"Organization-wide security awareness campaigns" "Leadership-endorsed security culture program" "Community threat intelligence sharing" "Non-punitive incident reporting culture"	"Monthly security newsletter (information only)" "Individual manager reminders" "Policy violation notices"	[10] [2][5][6][10][16]
Email Authentication Protocol Implementation	Organizational adoption and enforcement of email authentication standards to prevent spoofing	-SPF (Sender Policy Framework) deployment -DKIM (DomainKeys Identified Mail) implementation -DMARC (Domain-based Message Authentication) configuration -DMARC set to "reject" policy -Email verification procedures	-Individual email security features -End-user email clients -General email encryption -Technical spam filters without authentication protocols	"Organization-wide DMARC policy set to reject." "SPF and DKIM deployment across email infrastructure" "Email authentication verification procedures"	"Individual user email encryption" "Spam filter installation" "Email client security features"	[6] [5][11][16]
Regular Security Audits and Monitoring	Systematic periodic review of security controls, policies, and employee compliance related to phishing defenses	-Security audit programs -Compliance monitoring -Policy effectiveness review -Internal mail	-One-time audits -External compliance audits -Technical monitoring without	"Quarterly security audit of anti-phishing controls" "Continuous monitoring of internal mail	"Annual compliance audit for certification" "Automated IDS alerts" "Single security	[7] [10][16]

		monitoring -Network traffic analysis for phishing indicators -Continuous monitoring processes	organizational review -Automated alerts only	for suspicious activity" "Regular policy compliance reviews"	assessment"	
ITIL/Framework Adoption	Implementation of standardized IT service management or security frameworks to structure anti-phishing operations	-ITIL framework adoption -COBIT implementation -NIST framework usage -ISO 27001 compliance -Structured service management -Best practice frameworks	-Informal procedures -Custom approaches without a framework -Industry-specific standards -Compliance requirements only	"ITIL implementation for incident management" "COBIT framework for security governance" "NIST Phish Scale adoption for simulations"	"Custom incident response process" "Regulatory compliance only" "Industry-specific guidelines"	[9] [2][5][10]
Recruitment of Security-Skilled Personnel	Organizational hiring practices focused on acquiring staff with cybersecurity expertise to manage phishing defenses	-Hiring of security specialists -Recruitment of personnel with anti-phishing expertise -Building security teams -Skilled staff acquisition -IT security staffing initiatives	-General IT hiring -Outsourced services -Vendor support -Training existing staff	"Recruitment of CSIRT members with incident response expertise" "Hiring security analysts specialized in phishing detection." "Buildingan internal security operations team."	"Contracting external security vendor." "Training current IT staff." "Managed security service provider"	[5] [2][4][6]

Appendix 2: Organizational Measure Occurrence Summary

Rank	Measure	Number of Articles Mentioning	Percentage of Total (20 articles)	Primary Sources
1	Security Awareness Training	20	100%	[2][4][5][6][7]

	Programs			[8][11][12][13][14][15][16][21][22]
2	Incident Response Procedures	18	90%	[5][9][10][11][16][18][19]
3	Phishing Simulation Programs	16	80%	[4][9][12][14][15][17]
4	Security Policy Implementation	15	75%	[2][5][8][10][16][20]
5	Baseline Assessment and Metrics	14	70%	[4][9][12][14][15][17]
6	Phishing Reporting Mechanisms	12	60%	[9][10][13][16][17][18]
7	Employee Communication and Culture Building	10	50%	[2][5][6][10][16]
8	ITIL/Framework Adoption	9	45%	[2][5][10]
9	Multi-Factor Authentication (MFA) Policy	8	40%	[11][16]
10	Regular Security Audits and Monitoring	7	35%	[10][16]
11	Email Authentication Protocol Implementation	6	30%	[5][11][16]
12	Recruitment of Security-Skilled Personnel	5	25%	[2][4][6]

Appendix 3: Technology Controls Measure Classification Framework

Measure Class	Definition	Inclusion Criteria	Exclusion Criteria	Inclusion Case	Exclusion Case	Number of Occurrences

Content-Based Detection	Detection of phishing attacks by analyzing the content of emails or websites using natural language processing (NLP), semantic understanding, or deep learning methods. Content-based detection is particularly effective for enterprise phishing emails where malicious links may be embedded in otherwise legitimate-looking messages.	- Textual feature extraction (keywords, phrases) - Semantic or contextual language modeling - Deep learning for sequence analysis (e.g., LSTM, CNN)	- URL-only analysis without content processing - Solely human training programs without automated analysis	"LSTM-based email content classification to detect phishing patterns" "Semantic analysis of webpage text to classify phishing and legitimate sites"	“Techniques that depend only on human training programs or awareness campaigns, without automated content analysis.” “Systems that use header metadata, sender IP, or protocol-based features without examining the message body or webpage text.”	[27][29][30][31][34]
URL-Based Detection	Detection based on analyzing URL structures, lexical patterns, or statistical features to identify phishing links. These methods often rely on machine learning models to automatically classify URLs as malicious or legitimate.	- Lexical and structural URL analysis - Domain age verification and WHOIS checks - ML-based classification of URLs	- Content-only analysis - Manual URL checking without automated techniques	"Lexical and structural URL analysis for classification of phishing websites" "Multi-filter ML classification of URLs for phishing detection"	“Methods that analyze email or webpage content without considering the URL.” “Techniques relying solely on semantic text analysis, NLP, or LSTM-based content classification, ignoring URL structure and features.”	[25][26][28][31]
Hybrid Detection (URL + Content + Visual)	Detection using a combination of multiple features, including URL patterns, content, HTML structures, and visual cues. Hybrid systems integrate multiple detection signals for higher accuracy, especially against sophisticated phishing attacks that evade single-method detection.	- Multi-feature input from URL, content, and visual analysis - Sequence modeling and deep learning integration	- Single-source detection (URL only, content only) - Manual inspection without AI	"CNN + LSTM hybrid classification of website content, HTML structure, and visual features" "Analysis of both URL and webpage text in phishing detection"	“Detection methods that rely on a single source of features, such as URL-only, content-only, or visual-only analysis.” “Manual inspection or simple rule-based methods that do not combine multiple automated features.”	[27][31]

Behaviour-Based Detection	Detection of phishing attempts by analyzing user or system behavior, often through activity logs, anomaly detection, or sequence modeling. This approach is effective for insider-assisted or credential spear-phishing attacks.	- Monitoring user actions and system activity logs - Behavioral anomaly detection using ML/AI	- Content-only or URL-only detection - Manual observation without automated modeling	"Methods that ignore user or system activity patterns and focus only on static content or links." "Approaches that monitor data passively without detecting anomalies, such as manual audits or static logs."	“Spam filtering without behavior context” “phishing awareness Training programs”	[27][32]
Metadata-Based Detection	Detection based on metadata signals such as sender reputation, domain reputation, or SMTP/HTTP headers. Metadata analysis can identify phishing attempts even when content or URL analysis fails.	- Sender reputation scoring- Domain reputation analysis- Log correlation for anomalies	- Content-based or URL-only methods- Manual-only observation	"Correlation of domain and sender reputation to identify spear-phishing" "Analysis of SMTP/LDAP metadata for anomalous patterns"	“URL Semantic error detection” “Inspection of email content”	[32]
Rule-Based Detection	Detection using predefined rules, heuristics, or known patterns (e.g., typo-squatting, look-alike domains, SPF/DKIM validation). Rule-based detection is often used in enterprise settings as a complement to automated ML methods.	- Look-alike domain detection - SPF/DKIM validation - Typo-squatting or heuristic scoring	- Pure ML-only or AI-only systems - Human training without automated rules	"Detection of phishing using domain similarity and impersonation rules" "Validation of SPF/DKIM records for email authenticity"	“Regex-based spam filters only” “Auto links inspection using Deep Learning models”	[33]

LLM-Assisted Detection	Detection leveraging Large Language Models (LLMs) for semantic, contextual, or zero-shot phishing detection. LLMs can understand complex language patterns, making them effective for targeted phishing campaigns.	- Zero-shot or few-shot inference - Contextual and semantic analysis of email or web content	- Rule-based or traditional ML -only detection - Manual review only	- "Prompt-driven phishing classification using semantic analysis of emails" "Large language model inference for enterprise email security"	“Fully Automated Detection system” “Keyword-based spam filters”	[34]

Appendix 4: Technology Controls Measure Occurrence Summary

Rank	Measure Class	Number of Articles Mentioning	Percentage of Total Articles	Primary Sources
1	Content-Based Detection	5	50%	[27][29][30][31][34]
2	URL-Based Detection	4	40%	[25][26][28][31]
3	Hybrid Detection (URL + Content + Visual)	2	20%	[27][31]
4	Behaviour-Based Detection	2	20%	[27][32]
5	Metadata-Based Detection	1	10%	[32]
6	Rule-Based Detection	1	10%	[33]
7	LLM-Assisted Detection	1	10%	[34]

7. References

[1] A. Bhardwaj, V. Sapra, A. Kumar, N. Kumar, and S. Arthi, "Why is phishing still successful?," Computer Fraud & Security, vol. 2020, no. 9, pp. 15–19, Sep. 2020.

[2] E. D. Frauenstein and R. Von Solms, "Combating phishing: A holistic human approach," in Proc. IEEE Int. Conf. Inf. Secur. South Africa (ISSA), 2014, pp. 1–10.

[3] Tessian and Stanford University, "The Psychology of Human Error," 2020. [Online]. Available: https://www.tessian.com/research/the-psychology-of-human-error/

[4] D. Hillman and Y. Harel, "Evaluating organizational phishing awareness training on an enterprise scale," Comput. Secur., vol. 135, Article 103502, 2023.

[5] K. Althobaiti and S. Alsufyani, "A review of organization-oriented phishing research," PeerJ Comput. Sci., vol. 10, Article e2487, 2024.

[6] S. V. Pingle, "Prevention of Phishing Attacks: A Three-Pillared Approach," Issues Inf. Syst., vol. 21, no. 2, pp. 1-8, 2020.

[7] B. Naqvi et al., "Mitigation strategies against the phishing attacks: A systematic literature review," Comput. Secur., vol. 132, Article 103387, 2023.

[8] H. Shahbaznezhad, R. Dolan, and M. Rashidirad, "Employees' Behavior in Phishing Attacks: What Individual, Organizational, and Technological Factors Matter?" J. Comput. Inf. Syst., vol. 61, no. 6, pp. 539-550, 2021.

[9] L. Reinheimer et al., "Phishing in Organizations: Findings from a Large-Scale and Long-Term Study," arXiv preprint arXiv:2112.07498, 2021.

[10] K. Althobaiti, J. Jenkins, and K. Vaniea, "A Case Study of Phishing Incident Response in an Educational Organization," Proc. ACM Hum.-Comput. Interact., vol. 5, no. CSCW2, Article 338, Oct. 2021.

[11] M. A. Alotaibi and M. Ilyas, "Detection and prevention of spear phishing attacks: A comprehensive survey," Comput. Secur., Article 104172, Jan. 2025.

[12] G. Ho et al., "Understanding the Efficacy of Phishing Training in Practice," in Proc. IEEE Symp. Secur. Privacy (Oakland), 2025.

[13] M. Albladi and G. R. S. Weir, "Phishing Attacks: A Recent Comprehensive Study and a New Anatomy," Front. Comput. Sci., vol. 3, Article 563060, Jan. 2021.

[14] KnowBe4, "Phishing by Industry Benchmarking Report 2025," 2025.

[15] "Study Confirms Security Awareness Training Significantly Reduces Susceptibility to Phishing Attacks," HIPAA Journal, Jul. 2025.

[16] CISA, NSA, FBI, and MS-ISAC, "Phishing Guidance: Stopping the Attack Cycle at Phase One," Cybersecurity and Infrastructure Security Agency, Oct. 2023.

[17] "Retail Organization Sees 50-Fold Increase in Phishing Reporting with KnowBe4's Phish Alert Button and Training," KnowBe4 Case Study, Jul. 2025.

[18] M. Burkert, "SOC Phishing Playbook - A Comprehensive Guide," LinkedIn Article, Mar. 2023.

[19] M. Husák and J. Cegan, "PhiGARo: Automatic Phishing Detection and Incident Response Framework," in Proc. 9th Int. Conf. Availability, Reliability and Security (ARES), IEEE, 2014, pp. 295-302.

[20] G. Da Veiga and J. H. P. Eloff, "Information security policy development and implementation: The what, how, and who," Comput. Secur., vol. 69, pp. 77-97, Jun. 2016.

[21] K. Suzuki et al., "An Anti-phishing Training System for Security Awareness and Education Considering Prevention of Information Leakage," in Proc. IEEE Int. Conf. Consum. Electron. (ICCE-TW), 2019.

[22] A. A. Alsulami and N. S. Altamimi, "Evaluation of the Effective Anti-Phishing Awareness and Training in Governmental and Private Organizations in Riyadh," in Proc. IEEE Int. Conf. Inf. Commun. Syst. (ICICS), 2018.

[23] M. M. Al-Daeef, N. Basir, and M. M. Saudi, "Security Awareness Training: A Review," in Proc. World Congr. Eng. (WCE), London, U.K., Jul. 2017, vol. I.

[24] J. Whitman, A. El-Karim, P. Nandakumar, F. Ortega, L. Zheng, "Cost-Effective Cybersecurity Training Solutions for SMEs", Dec. 2024

[25] Muhammad Usman Javeed, S. M. Aslam, Hafiza Ayesha Sadiqa, and M. Akram, "Phishing Website URL Detection Using a Hybrid Machine Learning Approach," *ResearchGate*, Jun. 15, 2025. https://www.researchgate.net/publication/392704406_Phishing_Website_URL_Detection_Using_a_Hybrid_Machine_Learning_Approach (accessed Jan. 13, 2026).

[26] G. B. Mohammad, S. Shitharth, and P. R. Kumar, "Integrated machine learning model for an URL phishing detection," International Journal of Grid and Distributed Computing, vol. 14, no. 1, pp. 513–529, 2020, doi: https://www.researchgate.net/profile/Puranam-Revanth-Kumar/publication/352994631_Integrated_Machine_Learning_Model_for_an_URL_Phishing_Detection/links/60e303e2458515d6fbfd72f0/Integrated-Machine-Learning-Model-for-an-URL-Phishing-Detection.pdf.

[27] D. He, X. Lv, X. Xu, S. Chan, and K.-K. R. Choo, "Double-Layer Detection of Internal Threat in Enterprise Systems Based on Deep Learning," *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 4741–4751, 2024, doi: https://doi.org/10.1109/tifs.2024.3372771.

[28] B. B. Gupta, Akshat Gaurav, and K. T. Chui, "Convolution neural network (CNN) based phishing attack detection model for e-business in enterprise information systems," *AIS Electronic Library (AISeL)*, 2023. https://aisel.aisnet.org/iceb2023/71/ (accessed Jan. 11, 2026).

[29] M. Nabeel, Enes Altinisik, H. Sun, I. Khalil, H. W. Wang, and T. Yu, "CADUE: Content-Agnostic Detection of Unwanted Emails for Enterprise Security," pp. 205–219, Oct. 2021, doi: https://doi.org/10.1145/3471621.3471862.

[30] Q. Li, M. Cheng, J. Wang, and B. Sun, "LSTM Based Phishing Detection for Big Email Data," *IEEE Transactions on Big Data*, vol. 8, no. 1, pp. 278–288, Feb. 2022, doi: https://doi.org/10.1109/tbdata.2020.2978915.

[31] Moruf Akin Adebowale, K. T. Lwin, and M. A. Hossain, “Intelligent phishing detection scheme using deep learning algorithms,” *Journal of Enterprise Information Management*, vol. 36, no. 3, pp. 747–766, Jun. 2020, doi: https://doi.org/10.1108/jeim-01-2020-0036.

[32] G. Ho *et al.*, “Detecting Credential Spearphishing Attacks in Enterprise Settings Detecting Credential Spearphishing Attacks in Enterprise Settings,” 2017. Available: https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-ho.pdf

[33] Yuosuf Al-Hamar, Hoshang Kolivand, Mostafa Tajdini, T. Saba, and V. Ramachandran, “Enterprise Credential Spear-phishing attack detection,” *Computers & Electrical Engineering*, vol. 94, pp. 107363–107363, Aug. 2021, doi: https://doi.org/10.1016/j.compeleceng.2021.107363.

[34] J. Zhang, P. Wu, J. London, and D. Tenney, “Benchmarking and Evaluating Large Language Models in Phishing Detection for Small and Midsize Enterprises: A Comprehensive Analysis,” *IEEE Access*, vol. 13, pp. 28335–28352, 2025, doi: https://doi.org/10.1109/access.2025.3540075.

[35] D. Mercuri, “Enhancing Cybersecurity Awareness: Mitigating Phishing Risks for Employees in a Small Company,” Bachelor’s thesis, Laurea University of Applied Sciences, Business Information Technology, Helsinki, Finland, May 2025. Accessed: Dec. 12, 2025. [Online]. Available: https://www.theseus.fi/bitstream/handle/10024/891995/Mercuri_Daniele.pdf?sequence=2

[36] I. A. Shaik, “Hybrid threat detection systems: A synergistic approach to modern cybersecurity,” European Journal of Computer Science and Information Technology, vol. 13, no. 43, pp. 62–69, 2025, doi: 10.37745/ejcsit.2013/vol13n436269.