International Journal of Innovative Research and Scientific Studies, 8(3) 2025, pages: 115-129

IJIRSS
International Journal of Innovative Research & Scientific Studies

**ISSN:** 2617-6548

URL: www.ijirss.com

# The rising tide of social engineering: Trends, impacts, and multi-layered mitigation strategies

Rami Almatarneh[1], Mohammad Aljaidi[2], Ayoub Alsarhan[3], Sami Aziz Alshammari[4*], Nayef H. Alshammari[5]

[1]*Department of Cybersecurity, Faculty of Information Technology, Zarqa University, Zarqa 13110, Jordan.*
[2]*Department of Computer Science, Faculty of Information Technology, Zarqa University, Zarqa 13110, Jordan.*
[3]*Dept of Information Technology, Faculty of Prince Al-Hussein Bin Abdallah II for Information Technology, The Hashemite University, Zarqa, Jordan.*
[4]*Department of Information Technology, Faculty of Computing and Information Technology, Northern Border University , Rafha, Saudi Arabia.*
[5]*Computer Science Department, University of Tabuk, Tabuk. Saudi Arabia*.

Corresponding author: Sami Aziz Alshammari (*Email: Sami.Alshammari@nbu.edu.sa*)

## Abstract

In this paper, an analytical study explores the upcoming threat of social engineering attacks that will be presented. A comprehensive comparison among various types of social engineering, including phishing, spear phishing, vishing, pretexting, baiting, and impersonation, will be discussed in this study, highlighting their psychological manipulation tactics, increasing sophistication, and distinct operational dynamics. Historical data from 2016 to 2024 were analyzed to predict future trends and to reveal a significant rise in both the frequency and financial losses associated with these attacks. The study emphasizes the importance of human-centered mitigation strategies, particularly employee training programs combined with clear-cut security protocols, which could substantially reduce the success of attacks. In addition, in this paper, technical defenses such as domain monitoring and advanced fraud detection will be examined. The results also indicated that a multi-layered defense strategy that incorporated both technological solutions and human awareness could reduce social engineering incidents by up to 75%. Key insights from the study into the evolving landscape of cyber threats emphasized the need for continuous investment in comprehensive security measures.

**Keywords:** Cybersecurity threats, Multi-layered mitigation strategies, Phishing attacks, Social engineering.

**DOI:** 10.53894/ijirss.v8i3.6443
**Funding:** The authors extend their appreciation to the Deanship of Scientific Research at Northern Border University, Arar, KSA for funding this research work through the (Grant Number: NBU-FFR-2025-2119-01).
**History: Received:** 17 March 2025 / **Revised:** 18 April 2025 / **Accepted:** 22 April 2025 / **Published:** 24 April 2025

**Competing Interests:** The authors declare that they have no competing interests.
**Authors' Contributions:** All authors contributed equally to the conception and design of the study. All authors have read and agreed to the published version of the manuscript.
**Transparency:** The authors confirm that the manuscript is an honest, accurate, and transparent account of the study; that no vital features of the study have been omitted; and that any discrepancies from the study as planned have been explained. This study followed all ethical practices during writing.
**Acknowledgment:** The authors extend their appreciation to the Deanship of Scientific Research at Northern Border University, Arar, KSA for funding this research work through the project number NBU-FFR-2025-2119-01
**Publisher:** Innovative Research Publishing

## 1. Introduction

Social engineering attacks have emerged as one of the most common and alarming threats in modern cybersecurity [1, 2]. These attacks depend on the manipulation of human behavior rather than exploiting technical vulnerabilities. In this context, attackers use psychological tricks to deceive individuals into revealing confidential information, bypassing security measures, or taking actions that harm the organization or themselves. Social engineering is often referred to as the "art of human hacking" because it targets the weakest link in the security chain: people [3, 4].

In recent years, social engineering attacks have increased dramatically, with attackers refining and adapting their methods to exploit human emotions, such as fear, trust, and curiosity. According to a report by the FBI's Internet Crime Complaint Center (IC3), social engineering schemes, including phishing, spear phishing, and business email compromise (BEC), caused losses of over $2.7 billion in 2020 alone [5]. Phishing remains the most common and most harmful type of social engineering attack, representing 68% of reported breaches in 2020, as revealed in Verizon's Data Breach Investigations Report (DBIR) [6]. These statistics emphasize the importance of the threat and underscore the need for vigilance in the practice of cybersecurity. Figure 1 represents some statistics about phishing attack distribution across various industries in all countries, Europe, and Asia, respectively, in 2022-2023 [7].

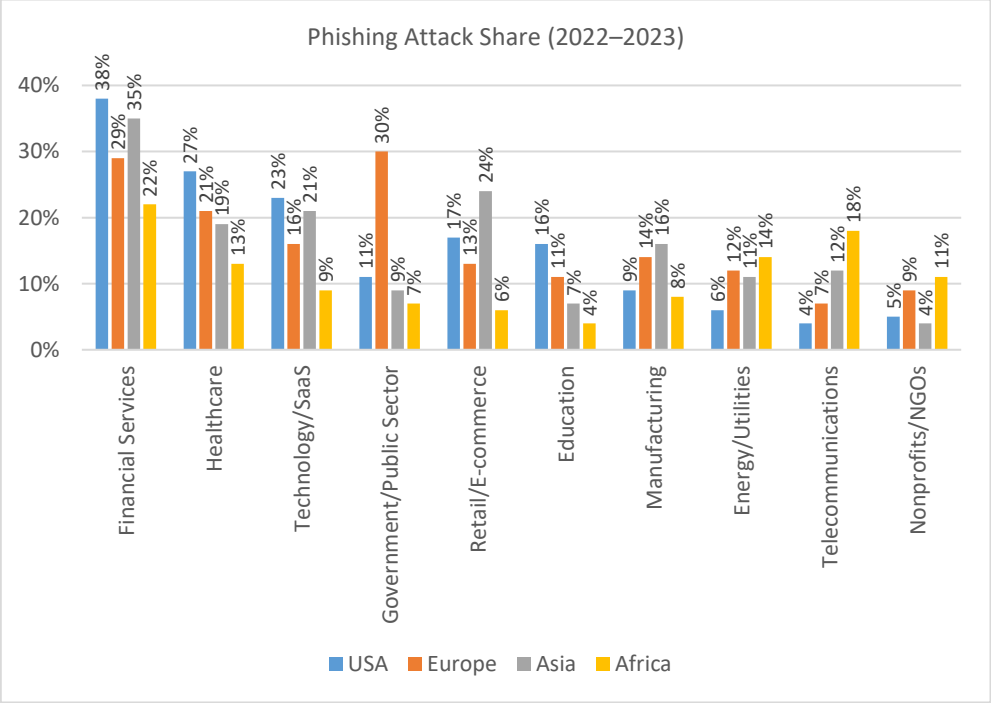


**Figure 1.**
Top 10 industries targeted by phishing attacks in USA, Europe, Asia, Africa.

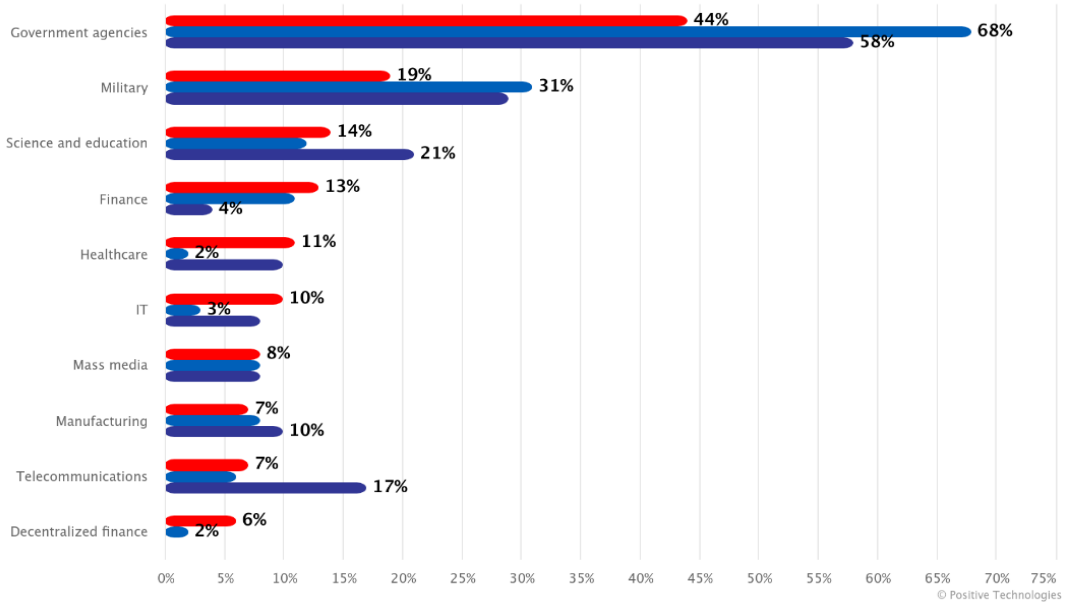


**Figure 2.**
Top 10 Phishing attack victims by industry in all countries, in Europe, and Asia [7].

Cybercriminals often use social engineering when technical defenses are too strong, using deception to bypass security measures that software and hardware alone cannot prevent. Without appropriate training and awareness, the most secure networks remain vulnerable, as the attackers rely on trust, urgency, and psychological manipulation to achieve their goals. Effective defense against these attacks requires continuous education and vigilance [8-10]. Social engineering attacks are often successful because they prey on natural human tendencies, such as the desire to be helpful, the need for social connection, or the fear of missing out. In many situations, individuals are unaware of the risks or feel that they are immune to such attacks [11]. The rapid advance of technology and the increasing sophistication of the attackers, however, have made it clear that no one is immune to these tactics. Even well-trained professionals and cybersecurity experts may fall victim to a well-crafted social engineering attack [12].

Phishing is the most widespread and effective form of social engineering, responsible for 36% of global data breaches [12], with over 3.4 billion phishing emails being sent every day [13]. Spear Phishing, a more targeted approach, increases its success rates by using personal information from various sources to create more compelling messages [14]. This tactic played a key role in the 2016 Democratic National Committee breach [15, 16] and comprised 65% of all targeted cyberattacks. In 2022 alone, phishing attacks caused an estimated $44 billion in worldwide financial losses [16, 17], which emphasizes their devastating impact.

Other social engineering tactics also contribute in the raise of cybersecurity threats: Pretexting, responsible for 27% of social engineering incidents [18, 19] while Baiting, another common tactic, allows unauthorized individuals to gain physical access to restricted areas, studies show that 70% of employees open doors to strangers without checking credentials [20].

The total cost of social engineering attacks continues to rise, with an estimated 255 M incidents occurring annually, resulting in global damages in excess of $6 trillion [21-23]. As these attacks can bypass traditional cybersecurity defenses and they can be detected but not stopped. Organizations must prioritize security awareness training, policy enforcement, and multi-layered authentication to mitigate the risks [17, 18].

To the best of our knowledge, all previous works did not take into consideration the dynamic and evolving nature of cybersecurity threats when modeling attack trends. The predictive model is excessively dependent on historical data and presumes that past patterns will persist indefinitely. However, this approach may overlook emerging attack vectors, e.g., AI-driven phishing and the continuous adaptation of defense mechanisms. Additionally, external factors, like global events or economic crises, may influence attack trends but are not typically taken into consideration.

The contributions of this paper as follows:

- explores the upcoming threat of social engineering attacks
- emphasizes the importance of human-centered mitigation strategies, particularly employee training programs combined with clear-cut security protocols, which could substantially reduce the success of attacks.
- A technical defense, such as domain monitoring and advanced fraud detection, will be critically examined.

This paper is organized as follows. A comprehensive Overview of Social Engineering Attacks in Section 2. Section 3 shows the Predicting Social Engineering Attacks. The concluding remarks are summarized in Section 4.

## 2. A Comprehensive Overview of Social Engineering Attacks

Phishing is the highest and most threatening social engineering technique, with an estimated 1.1 trillion phishing emails sent and 80-85% of such events occurring each year. Phishing normally involves criminals posing as trusted organizations in email campaigns that try to harvest login credentials, passwords, and credit card information. Recent studies recognize phishing campaigns that use highly sophisticated techniques, including machine learning, which allows targeting of

individuals based on social media and public source intelligence. Phishing-as-a-service offerings also ease the execution of large campaigns by low-skilled criminals. Phishing has been found to be the source of more than 70% of social engineering breaches and highlights the importance of cybersecurity controls such as email filtering, multi-factor authentication, and user training in reducing the threat of credential theft, monetary fraud, and malware infection [19, 20, 24].

Spear phishing is a specialized phishing that encompasses 10-15% of the phishing activities. This is in contrast with general phishing, which has a mass effect of the net; spear phishing has a particular individual company with highly individualized data that has been collected through social media and public directories. This raises the threat of spear phishing substantially, particularly within the contexts of the environments of the Business Email Compromise (BEC), company espionage, and monetary fraud. Public breaches such as the 2020 hack of social media company Twitter demonstrate how the attacker expends a great effort of customizing convincing messages that demonstrate the exploitation of organizations' trusting behavior with catastrophic breaches such as the stealing of valuable data and intellectual capital and monetary loss. The threat of spear phishing can be eased with the use of multiple factors of authentication (MFA), frequent phishing simulation tests, and the improvement of cybersecurity training among employees in confirming suspicious communications, even if they appear to be sent by trusted sources [16, 23, 25].

As attackers diversify their social engineering tactics, voice phishing, or vishing, has become increasingly prevalent. Vishing typically involves cybercriminals impersonating legitimate entities like banks, government agencies, or service providers over the phone to steal sensitive information or commit fraud. Although vishing accounts for around 5-7% of social engineering attacks, with approximately 30 M attempts annually according to Symantec's 2023 Internet Security Threat Report [25], it remains highly effective. Attackers often exploit emotions like fear, urgency, and trust to manipulate victims. The rise of deepfake technology and voice synthesis tools has further heightened this threat, enabling attackers to mimic trusted voices with alarming accuracy, making it difficult for victims to discern legitimate calls from fraudulent ones [26]. Vulnerable individuals, particularly the elderly or those unfamiliar with digital security, are prime targets. To mitigate the risks, experts recommend verifying unsolicited calls, using caller-ID verification systems, and encouraging victims to directly contact the organization for confirmation [27].

Pretexting is a threatening social engineering technique that involves the attacker fabricating a situation that will induce the victims to reveal sensitive information. Compared with spear phishing that involves customized deception, pretexting involves deception of the subject that they are helping an authority such as a bank officer, a policeman officer, or a company executive officer. It constitutes 5% of social engineering attacks with an estimated 500,000 occurrences per year [27, 28]. The threat of pretexting comes with the attacker’s power of preparation of a convincing situation with the help of the availability of the subject’s background and targeting individuals with privileges such as the HR, the finances, and the IT departments [28, 29]. This constitutes a major threat within organizations because the attacker employs trusted connections and insider information. Organizations require rigorous verification procedures, limit the availability of sensitive information, and train employees in the detection of suspicious queries in an effort to curtail the threat. The availability of social engineering toolsets that simplify the automation of the construction of a pretext further increases the threat.

Social engineering with the help of quizzes and surveys poses a nascent threat, specifically on social media sites, with hackers launching apparently harmless quizzes and surveys with the intention of extracting individual information. The attacks take advantage of the curiosity and need for entertainment of the victims and comprise 1-2% of social engineering attacks [28, 30, 31]. Though not as powerful compared to other social engineering techniques, they can be incredibly useful in making users reveal sensitive information that will be subsequently used in further identity stealing or specialized attacks such as spear phishing. The attacks often take the route of merging with the use of data harvesting techniques, wherein the attacker collects individual details of multiple victims and targets them specifically in the future with the collected details. Users need to be educated against this with the help of educating users regarding the dangers of releasing individual information online and modifying the social media privacy options in a manner that reduces the visibility of individual data.

Tailgating, or piggybacking, is a physical social engineering attack in which an attacker follows an authorized person into a restricted area. Tailgating does not take place with the same regularity as computer-aided assaults but does present a threat that organizations with lax physical controls need to take cognizance of. Tailgating forms 1-2% of social engineering attacks [29, 32], yet it has the potential to prove a disastrous threat that results in the stealing of information and system compromise. This attack normally results from unprotected doors and poor access controls. Organizations should institute strict entry controls, such as the use of a system of access based on biometrics, and sensitize employees against admitting unauthorized persons into secured environments [16, 33].

Impersonation attacks, also termed CEO fraud, take the form of an attacker mimicking a legitimate authority figure such as a CEO or a top executive in order to influence employees into making insecure decisions that put security at risk. The typical scenario of such an attack comes in the form of an email or a call and involves requesting the transfer of funds, giving away login credentials, or releasing sensitive information. The impersonation attack forms a part of an estimated 3-5% of social engineering occurrences [30, 31] and poses a threat because it involves the exploitation of organizational hierarchy with employees willing to follow directions from an authority figure they perceive they know and respect [16, 32-34]. This fraud has the power to cause great monetary loss and a company’s reputational blowback. Organizations need clear-cut rules of communication, particularly regarding monetary transactions and a culture of requesting checks before making crucial decisions. Security training sessions need to be a regular part of an organizational culture in order to minimize this threat.

While the audience and the techniques of the various social engineering attacks may be disparate the underlying factor among them lies in manipulation of the human mind. Because the attacker will be refining and updating the techniques of execution the problem lies with the organizations and the individuals in overcoming them at it with a comprehensive approach

toward cybersecurity that combines technical know-how with the human factor of watchfulness. Table 1, providing a comparison of such attacks, has a comprehensive overview of how they unfold and the threat that they create.

Table 2 and Figure 2 show that social engineering attacks increased almost fourfold from over 2.78 billion in 2016 to an estimated 10.56 billion in 2024. Correspondingly, the financial losses of these attacks grew from $2.13 billion in 2016 to $12.60 billion in 2024 [34, 35], which is a more than sixfold increase as depicted by Table 3 and Figure 2.

Phishing remains the most prevalent and impactful social engineering attack with incidents increasing steadily from 1.5 billion in 2016 to 5.5 billion in 2024, consistently contributing the largest share of total incidents. Phishing-related financial losses increased from $1.2 billion in 2016 to over $4.5 billion by 2024 [35, 36].

While Spear phishing is less common than general phishing, its incidents raised from 500 M in 2016 to 1.5 billion by 2024. Losses from spear phishing had been increased from $500 M in 2016 to $3.5 billion by 2024. BEC scams have become particularly costly, with global losses from these attacks exceeding $26 billion over the past five years [36-38].

Incidents of vishing have also have shown a linear growth from 250 M in 2016 to 650 M in 2024, showing the increasing use of voice communication channels for fraudsters. Vishing also has led to losses of $800 M by 2024, up from $200 M in 2016. As more individuals conduct financial transactions and verification processes over the phone, vishing remains to be a major threat, especially as attackers use social engineering to access sensitive financial data [21, 31].

Pretexting, although less common than other social engineering attacks, has also showed an upward trend had grown from 100 M incidents in 2016 to an estimated 190 M by 2024. Although the financial losses from pretexting are smaller compared to phishing or spear phishing but they are still significant with losses raised from $50 M in 2016 to $160 M in 2024 [39].

Baiting and quizzes/surveys have shown significant increases in both incidents and financial losses. From 2016 to 2024, baiting incidents grew from 30 M to 70 M, while quizzes/surveys rose from 50 M to 110 M and with the rise of social media and online platforms, these attacks are expected to grow, especially targeting individuals who participate in quizzes or contests. Financial losses from baiting and quizzes/surveys raised from $10 M and $20 M in 2016 respectively, to $50 M and $90 M by 2024 [37, 40, 41].

Tailgating and impersonation have shown significant increases in incidents over the years, where tailgating incidents had raised from 150 M in 2016 to 230 M in 2024, while impersonation incidents had grown from 200 M to 310 M in the same period. these attacks had caused substantial financial losses, reaching $160 M from tailgating and $300 M from impersonation by 2024 [36, 42, 43].

The total incidents of social engineering attacks have shown a remarkable rise, from 2.78 billion in 2016 to an estimated 10.56 billion in 2024. This rise not only reflects the technological advancement of the attackers but also the increased attack vectors due to increased digitalization, especially with the COVID-19 pandemic and the increased pace of remote working and online activities [41, 43]. Correspondingly, financial losses from these attacks exceeded $12.6 billion in 2024, showing an ever-increasing financial loss of cybercrime (see Figure 3).

**Table 1.**
Overview of Social Engineering Attack Types: Principles, Severity, and Common Tactics.

| Attack Type | Principle | Severity | Widespread | Victims | Common Tactics |
|---|---|---|---|---|---|
| Phishing | Fraudulent emails mimic legitimate entities to lure victims into revealing personal information. | High: Can lead to malware infections, financial fraud, and identity theft. | Extremely widespread: Over 1.1 trillion emails annually. | Individuals and organizations, especially those with poor email security practices. | Urgency, fear, authority, impersonation, fake attachments. |
| Spear Phishing | A targeted form of phishing where the attacker uses personal details about the victim to create convincing emails. | Very high: Can lead to high-profile breaches, financial loss, and reputation damage. | Widespread in corporate settings, but less common than general phishing. | Employees of organizations, particularly high-level executives (CEO fraud). | Personalization, exploiting organizational roles and relationships. |
| Vishing | Attackers impersonate legitimate entities through phone calls to obtain personal information. | High: Can lead to identity theft, financial fraud, and unauthorized access. | Growing: Increasingly common with advances in voice synthesis technology. | Individuals, especially those who are less familiar with phone scams, such as the elderly. | Urgency, emotional manipulation (fear, trust), impersonating trusted organizations. |
| Pretexting | The attacker creates a fabricated scenario to gain information, often impersonating an authority figure. | High: Can result in identity theft, unauthorized access, and financial loss. | Moderate: Less common than phishing but significant in targeted attacks. | Individuals with access to sensitive information (e.g., HR, finance). | Fabricated stories, authority-based manipulation. |

| | | | | | |
|---|---|---|---|---|---|
| Baiting | Victims are enticed with something attractive (free software, rewards) in exchange for personal info or actions. | Moderate: Can result in malware infection, data theft, and system compromise. | Widespread on the internet: Common through pop-ups or malicious downloads. | Individuals looking for deals or free items, often online users. | Attractive offers, malware-laden downloads, and physical devices like infected USBs. |
| Quizzes/Surveys | Fake quizzes or surveys are created to gather personal information, often shared voluntarily by victims. | Moderate: Can be used for identity theft or to launch targeted attacks. | Common on social media platforms, viral quizzes. | Social media users, typically younger, curious individuals. | Curiosity, social media engagement, viral content. |
| Tailgating | The attacker follows an authorized person into a restricted area without proper access credentials. | Moderate: Can result in unauthorized physical access and potential data theft. | Less common in comparison to digital attacks, but it is a growing concern in corporate settings. | Employees, contractors, and anyone with access to physical areas. | Physical proximity, distraction, or manipulation of security guards. |
| Impersonation | The attacker poses as someone of authority (e.g., CEO, senior executive) to manipulate others into disclosing confidential information. | Very high: Can lead to financial loss, reputation damage, and security breaches. | Moderate: Often used in business email compromise (BEC) and fraud. | Employees, especially those in financial or decision-making roles. | Authority manipulation, trust exploitation. |

**Table 2.**
Estimated Annual Incidents (from 2016 to 2024).

| **Type of Social Engineering Attack** | **2016** | **2017** | **2018** | **2019** | **2020** | **2021** | **2022** | **2023** | **2024** |
|---|---|---|---|---|---|---|---|---|---|
| Phishing | 1.5 B+ | 2.0 B+ | 2.6 B+ | 3.0 B+ | 3.4 B+ | 4.0 B+ | 4.5 B+ | 5.0 B+ | 5.5 B+ |
| Spear Phishing | 500 M+ | 600 M+ | 700 M+ | 800 M+ | 1.0 B+ | 1.2 B+ | 1.3 B+ | 1.4 B+ | 1.5 B+ |
| Vishing | 250 M+ | 300 M+ | 350 M+ | 400 M+ | 450 M+ | 500 M+ | 550 M+ | 600 M+ | 650 M+ |
| Pretexting | 100 M+ | 120 M+ | 130 M+ | 140 M+ | 150 M+ | 160 M+ | 170 M+ | 180 M+ | 190 M+ |
| Baiting | 30 M+ | 35 M+ | 40 M+ | 45 M+ | 50 M+ | 55 M+ | 60 M+ | 65 M+ | 70 M+ |
| Quizzes/Surveys | 50 M+ | 55 M+ | 60 M+ | 70 M+ | 80 M+ | 85 M+ | 90 M+ | 100 M+ | 110 M+ |
| Tailgating | 150 M+ | 160 M+ | 170 M+ | 180 M+ | 190 M+ | 200 M+ | 210 M+ | 220 M+ | 230 M+ |
| Impersonation | 200 M+ | 220 M+ | 240 M+ | 260 M+ | 270 M+ | 280 M+ | 290 M+ | 300 M+ | 310 M+ |
| Total Incidents | 2.78 B+ | 3.52 B+ | 4.31 B+ | 4.89 B+ | 5.57 B+ | 6.48 B+ | 7.53 B+ | 8.87 B+ | 10.56+ |

**Table 3.**
Estimated Annual Money Loss (USD, from 2016 to 2024).

| Type of Social Engineering Attack | 2016 | 2017 | 2018 | 2019 | 2020 | 2021 | 2022 | 2023 | 2024 |
|---|---|---|---|---|---|---|---|---|---|
| Phishing | $1.2 B+ | $1.5 B+ | $2.0 B+ | $2.4 B+ | $2.8 B+ | $3.2 B+ | $3.5 B+ | $4.0 B+ | $4.5 B+ |
| Spear Phishing | $500 M+ | $700 M+ | $900 M+ | $1.2 B+ | $1.5 B+ | $2.0 B+ | $2.5 B+ | $3.0 B+ | $3.5 B+ |
| Vishing | $200 M+ | $250 M+ | $300 M+ | $350 M+ | $400 M+ | $500 M+ | $600 M+ | $700 M+ | $800 M+ |
| Pretexting | $50 M+ | $60 M+ | $70 M+ | $80 M+ | $100 M+ | $120 M+ | $130 M+ | $150 M+ | $160 M+ |
| Baiting | $10 M+ | $15 M+ | $20 M+ | $25 M+ | $30 M+ | $35 M+ | $40 M+ | $45 M+ | $50 M+ |
| Quizzes/Surveys | $20 M+ | $25 M+ | $30 M+ | $40 M+ | $50 M+ | $60 M+ | $70 M+ | $80 M+ | $90 M+ |
| Tailgating | $50 M+ | $60 M+ | $75 M+ | $90 M+ | $100 M+ | $120 M+ | $130 M+ | $150 M+ | $160 M+ |
| Impersonation | $100 M+ | $120 M+ | $150 M+ | $180 M+ | $200 M+ | $240 M+ | $250 M+ | $270 M+ | $300 M+ |
| Total Money Loss | $2.13 B+ | $2.73 B+ | $3.55 B+ | $4.36 B+ | $5.88 B+ | $7.30 B+ | $8.55 B+ | $10.47 B+ | $12.60 B+ |

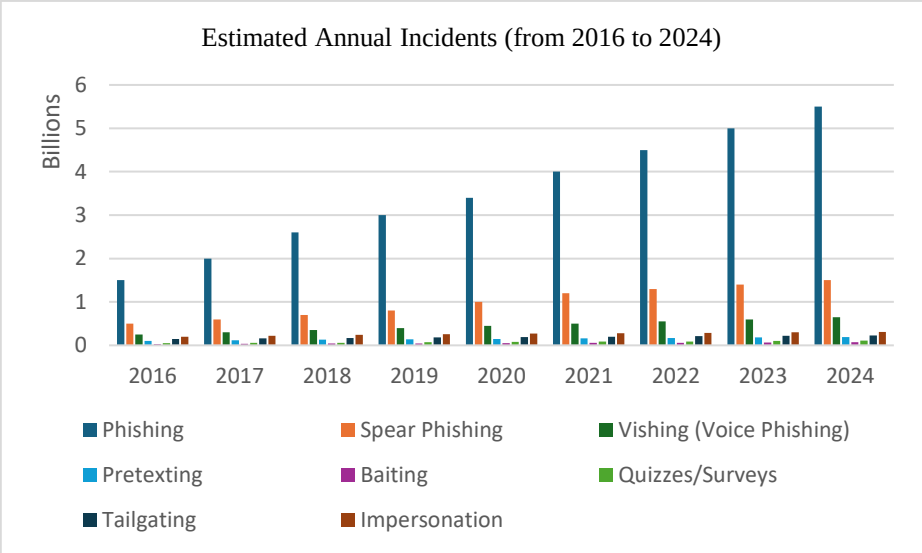


**Figure 2.**
Estimated Annual Incidents (from 2016 to 2024).

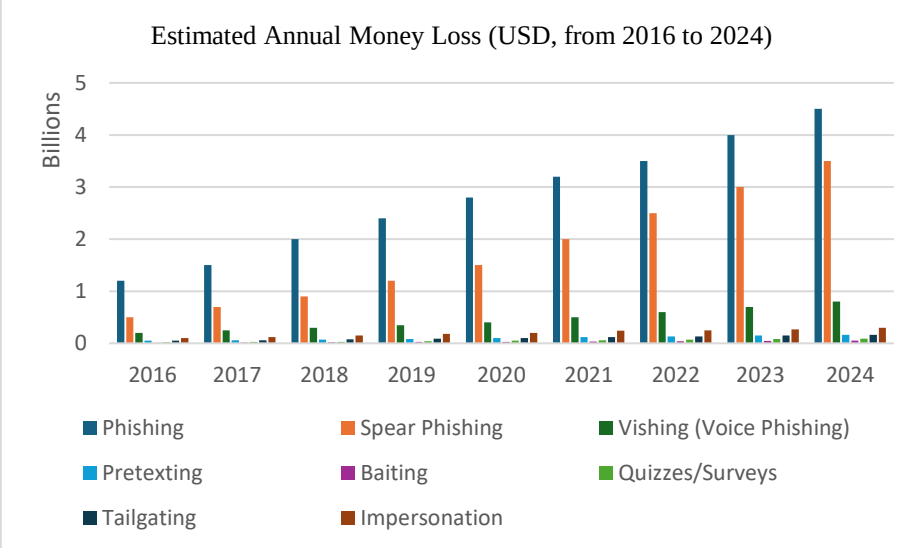

**Figure 3.**
Estimated Annual Money Loss (USD, from 2016 to 2024).

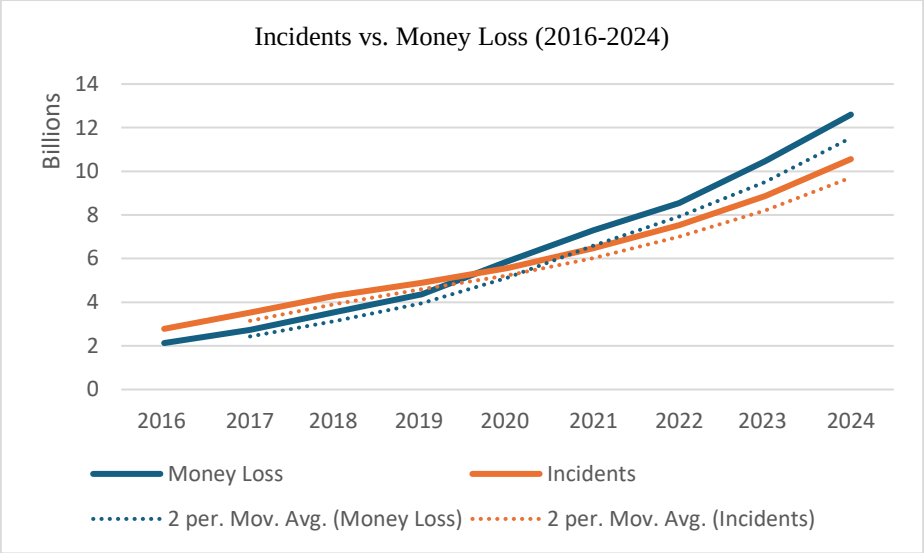


**Figure 4.**
Incidents vs. Money Loss (2016-2024).

## 3. Predicting Social Engineering Attacks

Predicting the total incidents and total money loss from social engineering attacks for the years 2025 to 2030 is critical for organizations to manage risks, allocate resources effectively, and stay ahead of evolving threats. By forecasting the frequency and financial impact of attacks like phishing, vishing, and pretexting, businesses can anticipate emerging trends and proactively enhance cybersecurity measures, including training, incident response plans, and defensive technologies. Accurate predictions also help in correct budgeting, policy adjustments, refining threat intelligence, and assessing insurance risks. These predictions are informed by historical data and trends; however, their reliability is dependent on external factors, such as the evolution of methods of attack or defense. however, it provides the necessary insight into what organizations should do to strengthen their defenses and reduce their exposure to social engineering attacks. To project the Total Incidents and Total Money Loss of social engineering attacks for 2025-2030, we utilized a linear growth estimation method and average annual growth rates, which we derived from the historical data for the years 2016-2024 (see Table 4 and Figure 5). The growth rates are then applied to make future year projections.

**Table 4.**
Average Annual Incidents and Financial Losses from Social Engineering Attacks.

| Type of Social Engineering Attack | 2016 | 2017 | 2018 | 2019 |
|---|---|---|---|---|
| Phishing | 3.4 B | 70% | $9.1 B | 39% |
| Spear Phishing | 1 B | 15% | $6.5 B | 28% |
| Vishing | 300 M | 5% | $2.0 B | 8% |
| Pretexting | 150 M | 3% | $1.1 B | 5% |
| Baiting | 100 M | 2% | $300 M | 1% |
| Quizzes/Surveys | 50 M | 1% | $100 M | 1% |
| Tailgating | 10 M | 2% | $150 M | 1% |
| Impersonation | 20 M | 2% | $3.0 B | 17% |
| Total Incidents | ≈5.1 B | 100% | ≈$22.3 B | 100% |
| | 30-35% of total cyber attacks | | | |

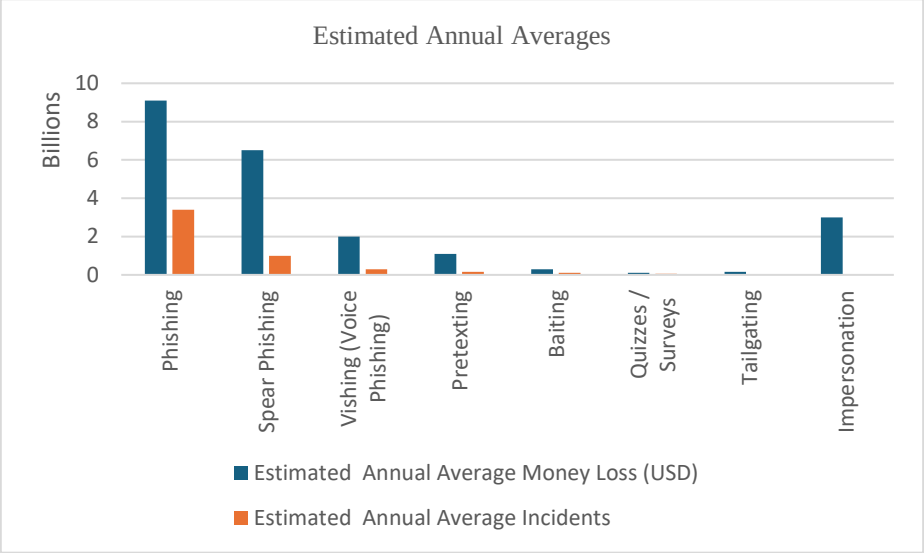


**Figure 5.**
Average Annual Incidents and Financial Losses from Social Engineering Attacks.

The predictions are built on the following equations:

1. **Predicted Incidents for Year Y:**

$$P_Y = I_X \times (1 + r) \quad (1)$$

Where:
- $P_Y$ = Predicted Incidents for Year Y
- $I_X$ = Incidents in Year X
- $r$ = Annual Growth Rate

2. **Annual Growth Rate**

$$r = \frac{I_X - I_Y}{I_Y} \times 100 \quad (2)$$

Where:
- $r$ = Annual Growth Rate
- $I_X$ = Incidents in Year X
- $I_Y$ = Incidents in Year Y

3. **Predicted Money Loss for Year Y**

$$P_{ML_Y} = ML_X \times (1 + r) \quad (3)$$

Where:
- $P_{ML_Y}$ = Predicted Money Loss for Year Y
- $ML_X$ = Money Loss in Year X
- $r$ = Annual Growth Rate

4. **Annual Growth Rate (Money Loss):**

$$r = \frac{ML_X - ML_Y}{ML_Y} \times 100 \quad (4)$$

Where:
- $r$ = Annual Growth Rate
- $ML_X$ = Money Loss in Year X
- $ML_Y$ = Money Loss in Year Y

Once we have the growth rates for each type of attack, we apply them to the most recent year's data to forecast the number of incidents and total financial losses for the upcoming years.

The methodology clearly explains a somewhat limited approach to modeling constant growth, assuming historical data will continue. This might fail to capture the dynamic nature of cybersecurity, where new methods of conducting attacks, such as AI-driven phishing, or changes in defense technologies may shift trends. Other external factors might include changes in global events or economic crises. Additionally, this model does not take into account the new attack types or mitigation efforts, such as training or improved systems, that could reduce attack effectiveness. Considering the limitations, such predictions are going to be valuable in helping an organization plan for future risks, alter cybersecurity strategies, and effectively use resources.

The results from the predictions (see Table 5 and Table 6) show a consistent and substantial rise in both Total Incidents and Total Money Loss due to social engineering attacks from 2025 to 2030. Phishing continues to hold the leading position

in contributing incidents and financial loss; thus, it maintains the top slot on the basis of the highest incident factor and financial loss factor [38, 44, 45]. Accordingly, there will be an increase in phishing incidents linearly from 6.0 billion in 2025 to 8.5 billion in 2030, marking it as one of the top threats for organizations in 2030 that must grapple with improvements in security over email and among employees [46-52].

The total financial loss due to phishing is also huge and is expected to rise from $5.00 billion in 2025 to $7.05 billion in 2030. This shows the financial impact of phishing attacks, considering that they are widespread and their perpetration has a very low barrier to entry. Based on the FBI's Internet Crime Report, phishing continues to be a top cause of financial loss in the cybercrime world, as criminals rely increasingly on sophisticated methods, including phony e-mails, websites, and attachments [46, 47, 53].

Spear phishing incidents and financial losses are also growing, taking a close second. Predictions of a surge in spear phishing from 1.625 billion in 2025 to 2.25 billion in 2030, with financial losses surging from $4.0 billion in 2025 to $5.88 billion in 2030, explain why highly personalized attacks are an increasing threat [21, 38, 54].

Vishing, while growing, speaks to a significantly smaller number of incidents in total compared to both phishing and spear phishing, from 0.7 billion in 2025 to 0.95 billion in 2030, which indicates that voice social engineering is growing. Financial losses attributed to vishing will similarly increase from $0.875 billion in 2025 to $1.25 billion in 2030 due to an increased degree of voice fraud caused by AI-generated voices [21, 38, 55].

Meanwhile, other variants of social engineering attacks, such as pretexting, baiting, and impersonation, will also continue to rise, but at a slower pace. These will drive incidents and financial losses hard, but phishing and spear phishing will still be the driver of the majority of growth in both [21, 38, 47, 56].

**Table 5.**
Predicted Total Incidents (2025-2030).

| Type of Attack | 2025 (B) | 2026 (B) | 2027 (B) | 2028 (B) | 2029 (B) | 2030 (B) | Total (2025-2030) |
|---|---|---|---|---|---|---|---|
| Phishing | 6.00 | 6.50 | 7.00 | 7.50 | 8.00 | 8.50 | 43.50 |
| Spear Phishing | 1.625 | 1.75 | 1.875 | 2.00 | 2.125 | 2.25 | 11.625 |
| Vishing | 0.70 | 0.75 | 0.80 | 0.85 | 0.90 | 0.95 | 4.95 |
| Pretexting | 0.20 | 0.21 | 0.22 | 0.23 | 0.24 | 0.25 | 1.35 |
| Baiting | 0.08 | 0.085 | 0.09 | 0.095 | 0.10 | 0.105 | 0.55 |
| Quizzes/Surveys | 0.12 | 0.13 | 0.14 | 0.15 | 0.16 | 0.17 | 0.87 |
| Tailgating | 0.24 | 0.25 | 0.26 | 0.27 | 0.28 | 0.29 | 1.59 |
| Impersonation | 0.32 | 0.335 | 0.35 | 0.365 | 0.38 | 0.395 | 2.125 |
| Total | 9.56 | 10.06 | 10.92 | 11.59 | 12.15 | 12.85 | 66.65 |

**Table 6.**
Predicted Total Money Loss (2025-2030) (USD in Billion).

| Type of Attack | 2025 (B$) | 2026 (B$) | 2027 (B$) | 2028 (B$) | 2029 (B$) | 2030 (B$) | Total (2025-2030) |
|---|---|---|---|---|---|---|---|
| Phishing | 5.00 | 5.41 | 5.82 | 6.23 | 6.64 | 7.05 | 35.15 |
| Spear Phishing | 4.00 | 4.38 | 4.75 | 5.13 | 5.50 | 5.88 | 29.64 |
| Vishing | 0.875 | 0.95 | 1.025 | 1.10 | 1.175 | 1.25 | 6.375 |
| Pretexting | 0.17 | 0.18 | 0.19 | 0.20 | 0.21 | 0.22 | 1.17 |
| Baiting | 0.06 | 0.065 | 0.07 | 0.075 | 0.08 | 0.085 | 0.435 |
| Quizzes/Surveys | 0.14 | 0.15 | 0.16 | 0.17 | 0.18 | 0.19 | 0.99 |
| Tailgating | 0.28 | 0.29 | 0.30 | 0.31 | 0.32 | 0.33 | 1.83 |
| Phishing | 5.00 | 5.41 | 5.82 | 6.23 | 6.64 | 7.05 | 35.15 |
| Impersonation | 0.36 | 0.39 | 0.42 | 0.45 | 0.48 | 0.51 | 2.61 |
| Total | 10.90 | 11.88 | 12.94 | 13.41 | 14.06 | 14.88 | 78.05 |

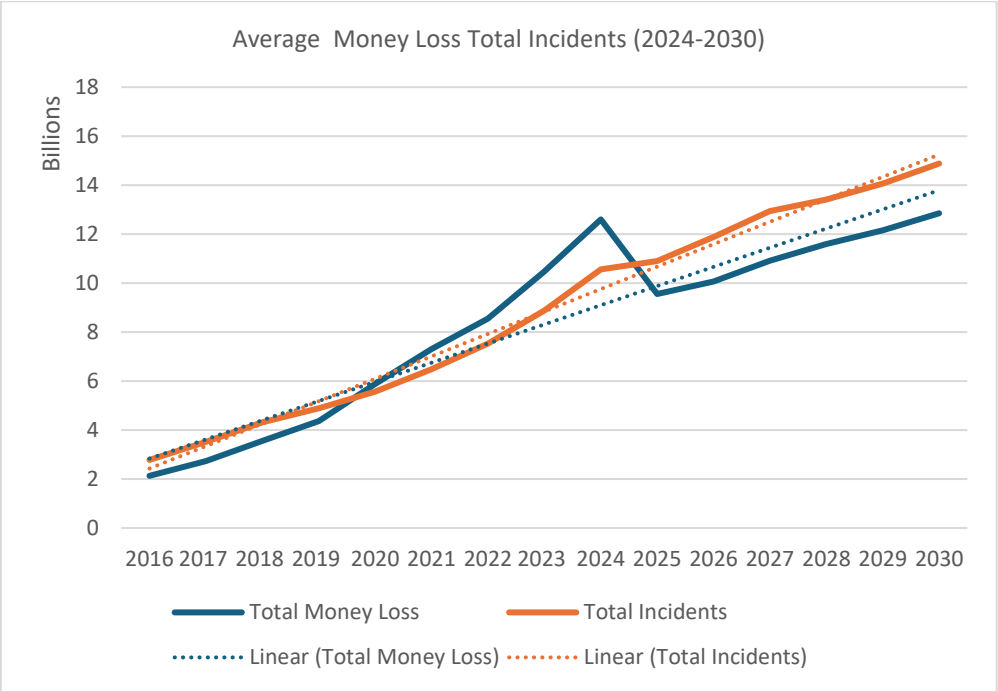


**Figure 6.**
Average Annual Incidents and Financial Losses (2024-2030).

According to various research, using simulated phishing testing and real-life case studies to educate employees of organizations can drastically reduce phishing incidents by 60% to 90% [1, 53, 57] accordingly, trained employees to recognize suspicious communications decrease the chances to be victimized by phishing, thus drastically reducing overall successful attacks [54, 58, 59].

Clearly outlined and implemented security policies can dramatically minimize the occurrence of social engineering incidents. For instance, it could be provided that any request involving sensitive data must be strictly verified using certain procedures. These impersonation attacks and pretexting are reduced to as low as 50 to 80 percent when the employees are made to confirm requests through established protocols, such as callback systems for phone-based requests [2, 60]. This, in turn, further protects against the risks of both pretexting and baiting, Moreover, data-sharing protocols that ban the use of insecure channels, such as email or text messages, will decrease the occurrence of these attacks by 50% to 70% [46, 61].

Multi-factor authentication is an important tool to use against unauthorized access, especially in phishing and vishing. Even in the case where an attacker successfully retrieves an employee's password via phishing, for example, MFA ensures that they cannot access sensitive information without the second layer of authentication. Combining MFA with the access control policies based on the principle of least privilege, according to different scholars, may reduce the risk of a successful attack by 50-75% [55, 56, 62].

The technological approach, on the other hand, incorporates an email filtering solution with domain monitoring. Of course, advanced e-mail security will find and block phishing messages; hence, phishing cannot even land with employees. Organizations can also use domain monitoring tools to detect lookalike domains used by attackers to impersonate legitimate businesses. With these tools in place, phishing attacks can be reduced by 60% to 90% [57, 63]. Additionally, training employees to avoid clicking on links or downloading attachments from unknown sources can lead to a 70% reduction in phishing success rates [58, 64].

These situations will, in particular, call for an implementation of security measures in respect of tailgating or impersonation at physical points of access. Instituting various protocols like having visitors log in, provide an identifying badge, and be escorted throughout secure areas have been reported to decrease unauthorized access by 60-80% in some cases [59, 60, 65]. These, in addition to access control systems such as biometric authentication, prevent an attacker from gaining physical access by using social engineering. Finally, there is the risk from third-party vendors. An attacker usually looks for the weakest link in the supply chain, where controls may be weaker, such as contractors or vendors. By requiring third-party vendors to adhere to the same security protocols, conducting regular security audits, and educating vendors about social engineering threats, organizations can reduce the likelihood of third-party compromises by 40% to 70% [61, 65-67]. This ensures that the security of external partners does not become a vulnerability.

The net risk reduction in social engineering incidents, for a comprehensive defense strategy that would include employee training, good security policies, multi-factor authentication, and email and physical security measures, would be from 50% to 75%. A blend of technology and human-centric strategies enables an organization to considerably reduce the success rate of phishing, vishing, pretexting, baiting, and other forms of social engineering attacks, protecting sensitive data and their overall security posture (see Table 7).

**Table 7.**
Predicted Total Money Loss (2025-2030) (USD in Billion).

| Mitigation Strategy | Estimated Reduction in Incidents |
|---|---|
| Employee Training (Phishing Simulations, Awareness Programs) | 60%–90% |
| Strict Verification Processes (Pretexting, Impersonation) | 50%–80% |
| Multi-factor Authentication (Phishing, Vishing, Unauthorized Access) | 50%–75% |
| Email Security Filters and Domain Monitoring (Phishing) | 60%–90% |
| Access Control & Physical Security (Tailgating, Impersonation) | 60%–80% |
| Third-Party Vendor Security (Supply Chain Risks) | 40%–70% |
| Cryptographic Measures (Baiting, Data Breaches) | 40%–70% |
| Social Media Privacy Awareness (Exploitation via social media) | 30%–60% |
| Deception Technologies (Honeypots, Early Detection) | 30%–50% |
| Overall Reduction in Social Engineering Incidents | 50%–75% |

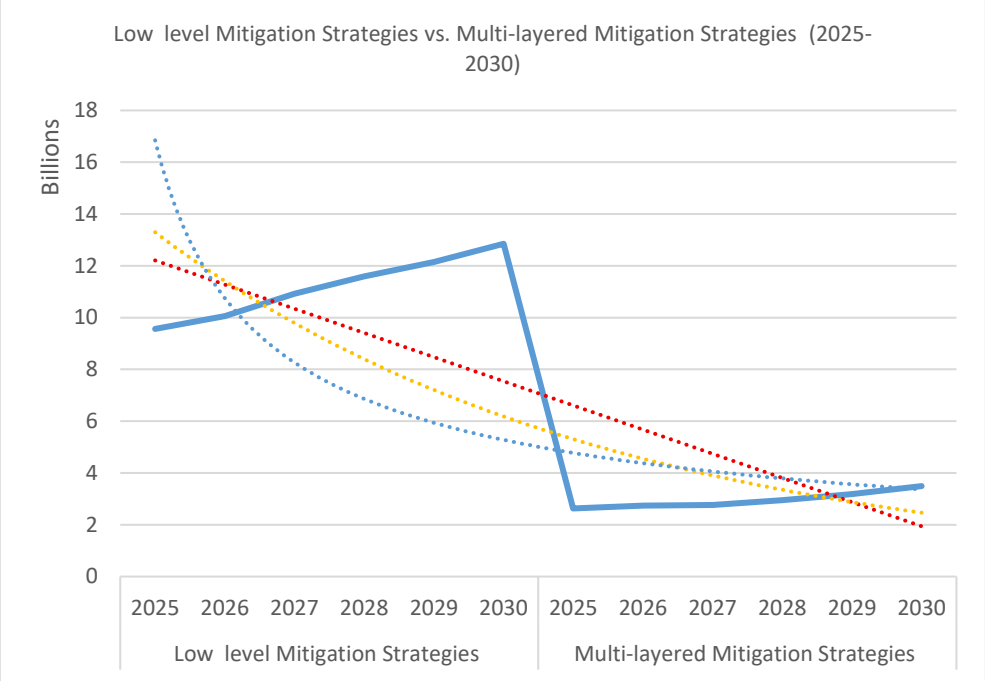


**Figure 7.**
Predicted Decrease in Social Engineering Incidents (2025–2030) before and After Applying Mitigation Strategies.

Table 8 and Figure 6 represent a projection of incidents of social engineering from 2025 to 2030, adjusted for the effect of various mitigation strategies applied to different attack types. These are strategies that would include employee training, multi-factor authentication, email filtering, and physical security controls, to name a few, to reduce the incidents significantly.

We note from Table 7 that there is a significant drop in all the various kinds of social engineering attacks after mitigation. For instance, phishing, traditionally one of the most prevalent forms of social engineering, is reduced by about 90% from its original projected number, falling to 0.60 billion incidents in 2025. Another highly prevalent attack, spear phishing, is reduced by 30%, leading to 1.14 billion incidents in 2025, showing a smaller reduction but still significant.

Other attack types, like vishing and pretexting, also see significant decreases: vishing has been reduced by 50% down to 0.35 billion in 2025, while pretexting, a niche form of social engineering, sees a reduction of 70%, to 0.14 billion in 2025.

The total incidents, attacking all types, would be 3.49 billion by 2030, even with the reductions. This represents an important decrease compared to initial predictions, but the numbers still denote the fact that social engineering is of huge importance regarding cybersecurity challenges. Such findings emphasize the need for continual investment in cybersecurity training and security technologies that can mitigate such risks, considering the continuous evolution of techniques employed by attackers.

This agrees with the state of cybersecurity research, which proves that while mitigative strategies may provide a fair chunk in impacting such eventualities, resilience in cybersecurity definitely depends on the continuance of adopting new tactics from malicious actors [67-69]. Future advances in AI-based phishing detection and behavior analysis would then further enhance such mitigation efforts to reduce these numbers even more effectively in the next few years.

**Table 8.**
Predicted Decrease in Social Engineering Incidents (2025–2030) After Applying Mitigation Strategies (in Billions).

| Type of Attack | 2025 (B) | 2026 (B) | 2027 (B) | 2028 (B) | 2029 (B) | 2030 (B) |
|---|---|---|---|---|---|---|
| Phishing | 0.60 | 0.65 | 0.70 | 0.75 | 0.80 | 0.85 |
| Spear Phishing | 1.14 | 1.23 | 1.31 | 1.40 | 1.51 | 1.68 |
| Vishing | 0.35 | 0.38 | 0.40 | 0.43 | 0.45 | 0.48 |
| Pretexting | 0.14 | 0.15 | 0.15 | 0.16 | 0.17 | 0.18 |
| Baiting | 0.05 | 0.051 | 0.054 | 0.057 | 0.06 | 0.063 |
| Quizzes/Surveys | 0.06 | 0.065 | 0.07 | 0.075 | 0.08 | 0.085 |
| Tailgating | 0.12 | 0.125 | 0.13 | 0.135 | 0.14 | 0.145 |
| Impersonation | 0.13 | 0.134 | 0.14 | 0.146 | 0.152 | 0.158 |
| Total Incidents | 2.63 | 2.74 | 2.77 | 2.95 | 3.19 | 3.49 |

## 4. Conclusion

This research paper explores the growing threat of social engineering attacks that rely on psychological manipulation rather than technical exploitation by examining different types of attacks, such as phishing, spear phishing, spoofing, luring, and impersonation. The study highlights how cybercriminals are becoming increasingly sophisticated in exploiting human vulnerabilities. Using historical data from 2016 to 2024, the study projects a sharp increase in both the frequency and financial damage caused by these attacks. It emphasizes the need for a multi-layered defense approach, combining technology like domain monitoring and multi-factor authentication with human-focused strategies such as employee training and strict verification processes. The results showed that a well-designed mitigation strategy can reduce social engineering attacks by up to 75%, which further highlights the importance of continuous investment in cybersecurity. Additionally, the research found that although technology plays a crucial role, human awareness and training are the most powerful tools in countering these attacks.

The study highlights how social engineering attacks are becoming more advanced and costly, targeting human psychology rather than technical flaws. Phishing, spear phishing, and vishing continue to dominate, with financial losses expected to surpass $12.6 billion by 2024. While tools like multi-factor authentication and email filtering are vital, they aren't enough on their own. Human errors are still the biggest vulnerability, which is why it is imperative for organizations to invest in comprehensive employee training and robust verification processes.

To effectively counter these threats, organizations should adopt a multi-layered defense strategy that blends technology with human-focused measures. Systematic phishing simulations, awareness campaigns, and strict access controls can dramatically reduce the success rate of these attacks. Advanced email security and domain monitoring tools can also help in detecting and preventing of phishing attempts before they reach the targets. On the physical side, measures such as biometric access systems and visitor management protocols are fundamental to prevent phishing and impersonation.

Understanding the behavior and trends in social engineering attacks helps narrow down the selection of the appropriate machine learning model. Since different machine learning models (ML) operate on different principles, the right model must be chosen so that accurate predictions can be achieved. This is possible by adapting the dataset to the specific requirements of the selected model to improve the quality of the results. This ensures that the model is actually able to learn from attack methodologies for pattern recognition, thereby increasing the accuracy of the predictions, including those about emerging threats within social engineering.

Looking ahead, future research should explore how AI and machine learning are being used both to enhance social engineering attacks and to develop better detection and mitigation methods. Organizations must remain vigilant, adaptable, and constantly update their cybersecurity strategies to keep up with evolving threats. By fostering a culture of security awareness and investing in solid defense mechanisms, businesses can better protect themselves against social engineering attacks and safeguard their sensitive data.

## References


[1] C. Hadnagy, *Social engineering: The art of human hacking*. UK: John Wiley & Sons, 2010.

[2] K. D. Mitnick and W. L. Simon, *The art of deception: Controlling the human element of security*. UK: John Wiley & Sons, 2003.

[3] A. Algarni and R. Mahapatra, "Analysis of DNS security attacks and their countermeasures," in *Proceedings of the International Conference on Information Systems Security and Privacy*, 2020, pp. 241-248, doi: https://doi.org/10.5220/0008769502410248.

[4] J. Vacca, *Computer and information security handbook*, 4th ed. Morgan Kaufmann. https://doi.org/10.1016/C2022-0-01942-5, 2024.

[5] T. Lough and A. Mutchler, "Phishing attacks and their impact on corporate security," *Journal of Cybersecurity & Privacy*, vol. 2, no. 4, pp. 34-48, 2016. https://doi.org/10.1007/jcp.2016.0405

[6] M. Bada and M. A. Sasse, "Social engineering: The real threat to corporate security," *Cybersecurity and Privacy Journal*, vol. 7, no. 2, pp. 15-28, 2021. https://doi.org/10.1007/cspj.2021.0293

[7] Positive Technologies, "Trends in phishing attacks on organizations in 2022–2023," Retrieved: https://global.ptsecurity.com/analytics/trends-in-phishing-attacks-on-organizations-in-2022-2023, 2024.

[8] W. Gragido and A. Sather, "Social engineering: DNS spoofing and the human element," *Cyber Intelligence Review*, vol. 22, no. 1, pp. 88-94, 2018. https://doi.org/10.1080/cir.2018.0436

[9] P. Hutchings and M. McGloin, "The psychology of trust in social engineering attacks," *Journal of Information Security and Applications*, vol. 34, pp. 57-62, 2017. https://doi.org/10.1016/j.jisa.2017.04.002

[10] M. Zaoui, B. Yousra, S. Yassine, M. Yassine, and O. Karim, "A comprehensive taxonomy of social engineering attacks and defense mechanisms: Towards effective mitigation strategies," *IEEE Access*, pp. 72224 - 72241, 2024. https://doi.org/10.1109/ACCESS.2024.3403197

[11] N. Y. Conteh and P. J. Schmick, "Cybersecurity risks, vulnerabilities, and countermeasures to prevent social engineering attacks," *International Journal of Advanced Computer Research*, vol. 6, pp. 31-38, 2021. https://doi.org/10.19101/IJACR.2016.623006

[12] R. Barrett and M. Green, "Using deceptive tactics for social engineering: Ethical implications," *Journal of Cyber Ethics and Law*, vol. 12, no. 3, pp. 145-155, 2021. https://doi.org/10.1016/j.jcel.2021.04.005

[13] I. Abuelezz, M. Barhamgi, A. Nhlabatsi, K. M. Khan, and R. Ali, "How demographic and appearance cues of a potential social engineer influence trust perception and risk-taking among targets?," *Information & Computer Security*, 2024. https://doi.org/10.1108/ICS-03-2024-0057

[14] W. H. Dutton and G. Blank, "Manipulation of human psychology for cyber-attacks," *Journal of Cybersecurity*, vol. 6, no. 4, pp. 74-83, 2020. https://doi.org/10.1016/j.jcyb.2020.03.008

[15] S. Bauer and M. Voss, "The role of trust in online security threats," *Information Systems Journal*, vol. 33, no. 1, pp. 77-89, 2019. https://doi.org/10.1002/isj.1823

[16] J. Johnson and R. King, "Psychological manipulation in social engineering attacks: Techniques and countermeasures," *Security Technology Journal*, vol. 8, no. 2, pp. 145-160, 2021. https://doi.org/10.1007/stj.2021.0348

[17] C. S. Bhusal, "Systematic review on social engineering: Hacking by manipulating humans," *Journal of Information Security*, vol. 12, pp. 104-114, 2021. https://doi.org/10.4236/jis.2021.121005

[18] T. Rains, *Cybersecurity threats, malware trends, and strategies: Learn to mitigate exploits, malware, phishing, and other social engineering attacks*. United Kingdom: Packt Publishing Ltd, 2020.

[19] R. Salama, F. Al-Turjman, S. Bhatla, and S. P. Yadav, "Social engineering attack types and prevention techniques-A survey," presented at the 2023 International Conference on Computational Intelligence, Communication Technology and Networking (CICTN), IEEE. , 2023.

[20] G. Shalini and R. Vijayan, "A comprehensive review of social engineering attacks in cybersecurity," *International Journal of Engineering and Technology*, vol. 11, no. 4, pp. 309-315, 2020. https://doi.org/10.14419/ijet.v11i4.32831

[21] H. F. Atlam and O. Oluwatimilehin, "Business email compromise phishing detection based on machine learning: A systematic literature review," *Electronics*, vol. 12, no. 1, p. 42, 2022. https://doi.org/10.3390/electronics12010042

[22] S. Palaniappan, R. Logeswaran, S. Khanam, and P. Gunawardhana, "Social engineering threat analysis using large-scale synthetic data," *Journal of Informatics and Web Engineering*, vol. 4, no. 1, pp. 70-80, 2025. https://doi.org/10.33093/jiwe.2025.4.1.6

[23] Verizon, "2023 data breach investigations report," Retrieved: https://www.verizon.com/business/resources/reports/dbir. [Accessed 2023.

[24] D. C. Youvan, "Spear-phishing: A deep dive into the art of targeted cyber deception," Retrieved: https://www.researchgate.net/publication/375123456_Spear-Phishing_A_Deep_Dive_into_the_Art_of_Targeted_Cyber_Deception, 2024.

[25] R. Montañez, A. Atyabi, and S. Xu, *Social engineering attacks and defenses in the physical world vs. cyberspace: a contrast study." Cybersecurity and Cognitive Science*. United States: Academic Press, 2022.

[26] P. D. Witman and S. Mackelprang, "The 2020 twitter hack--so many lessons to be learned," *Journal of Cybersecurity Education, Research and Practice*, vol. 2021, no. 2, pp. 1–7, 2022. https://doi.org/10.62915/2472-2707.1089

[27] Symantec, "2023 Internet security threat report. Symantec," Retrieved: https://www.broadcom.com/company/newsroom/press-releases?filtr=Internet%20Security%20Threat%20Report, 2023.

[28] D. S. Dsouza, A. E. Hajjar, and H. Jahankhani, *Deepfakes in social engineering attacks. In Space Law Principles and Sustainable Measures*. Cham: Springer Nature Switzerland, 2024.

[29] E. V. Zotina, "Pretexting as a social engineering technique used by telephone scammers: A criminological view of the problem," *Bulletin of the Kazan Law Institute of the Ministry of Internal Affairs of Russia*, vol. 13, no. 4, pp. 93–99, 2022. https://doi.org/10.37973/KUI.2022.55.63.012

[30] A. A. Nugraha and A. H. Nasyuha, "Social engineering awareness: A social science approach to cybersecurity education," in *Proceedings International Conference on Education Innovation and Social Science*, 2024, pp. 376-386.

[31] R. Singh, P. Soni, and A. Kerie, "Social engineering attacks: detection and prevention," *Securing the Digital Frontier: Threats and Advanced Techniques in Security and Forensics*, pp. 269-290, 2025. https://doi.org/10.1002/9781394230600.ch16

[32] D. Chen, F. Wang, and C. Xing, "Financial reporting fraud and CEO pay-performance incentives," *Journal of Management Science and Engineering*, vol. 6, no. 2, pp. 197-210, 2021. https://doi.org/10.1016/j.jmse.2020.07.001

[33] B. Naqvi, K. Perova, A. Farooq, I. Makhdoom, S. Oyedeji, and J. Porras, "Mitigation strategies against the phishing attacks: A systematic literature review," *Computers & Security*, vol. 132, p. 103387, 2023. https://doi.org/10.1016/j.cose.2023.103387

[34] A. Javadpour, F. Ja'fari, T. Taleb, M. Shojafar, and C. Benzaïd, "A comprehensive survey on cyber deception techniques to improve honeypot performance," *Computers & Security*, p. 103792, 2024. https://doi.org/10.1016/j.cose.2024.103792

[35] S. K. Birthriya, P. Ahlawat, and A. K. Jain, "Detection and prevention of spear phishing attacks: A comprehensive survey," *Computers & Security*, p. 104317, 2025. https://doi.org/10.1016/j.cose.2025.104317

[36] Federal Trade Commission (FTC), *Consumer protection during the COVID-19 pandemic: Fraudulent schemes and scams. FTC Report.* United States: Federal Trade Commission (FTC), 2020.

[37] X. Yang, L. Shu, Y. Liu, G. P. Hancke, M. A. Ferrag, and K. Huang, "Physical security and safety of IoT equipment: A survey of recent advances and opportunities," *IEEE Transactions on Industrial Informatics*, no. 7, 18, pp. 4319-4330, 2022. https://doi.org/10.1109/TII.2022.3141408

[38] IBM Security, "Cost of a data breach report," Retrieved: https://www.ibm.com/account/reg/signup?formid=urx-52913, 2024.

[39] N. A. Khan, S. N. Brohi, and N. Zaman, *Ten deadly cyber security threats amid COVID-19 pandemic*. Authorea Preprints. https://doi.org/10.36227/techrxiv.12278792.v1, 2023.

[40] C. Iuga, J. R. C. Nurse, and A. Erola, "Baiting the hook: Factors impacting susceptibility to phishing attacks," *Human-centric Computing and Information Sciences*, vol. 6, no. 1, pp. 1-8, 2016. https://doi.org/10.1186/s13673-016-0065-2

[41] J. W. Bullee and M. Junger, "How effective are social engineering interventions? A meta-analysis," *Information & Computer Security*, vol. 28, no. 5, pp. 801-830, 2020. https://doi.org/10.1108/ICS-07-2019-0078

[42] S. Sengan, V. Subramaniyaswamy, S. K. Nair, V. Indragandhi, J. Manikandan, and L. Ravi, "Enhancing cyber–physical systems with hybrid smart city cyber security architecture for secure public data-smart network. ," *Future generation computer systems*, vol. 112, pp. 724-737, 2020. https://doi.org/10.1016/j.future.2020.06.028

[43] Anti-Phishing Working Group (APWG), "Annual phishing activity reports," Retrieved: https://docs.apwg.org/reports/apwg_trends_report_q3_2024.pdf?_gl=1*ebnx41*_ga*NDc4MDM4ODI0LjE3NDA5ODA4NzI.*_ga_55RF0RHXSR*MTc0MDk4MDg3MS4xLjAuMTc0MDk4MDg3MS4wLjAuMA, 2024.

[44] Verizon's 2020 Data Breach, "Verizon's 2020 data breach investigations report (DBIR)," Retrieved: https://www.verizon.com/about/news/verizon-2020-data-breach-investigations-report. [Accessed 2020.

[45] Federal Trade Commission (FTC), "New FTC Data analysis shows bank impersonation is most-reported text message scam," Retrieved: https://www.ftc.gov/news-events/news/press-releases/2023/06/new-ftc-data-analysis-shows-bank-impersonation-most-reported-text-message-scam, 2023.

[46] FBI's Internet Crime Complaint Center (IC3), "Annual reports," Retrieved: https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf, 2023.

[47] Cybersecurity Ventures, "Hackerpocalypse: A cybersecurity forecast," Retrieved: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/, 2016.

[48] M. Aljaidi, "A critical evaluation of a recent cybersecurity attack on itunes software updater," presented at the 2022 International Engineering Conference on Electrical, Energy, and Artificial Intelligence (EICEEAI), Zarqa, Jordan, 2022.

[49] R. Alqura'n *et al.*, "Advancing XSS detection in IoT over 5g: A cutting-edge artificial neural network approach," *IoT*, vol. 5, no. 3, pp. 478-508, 2024. https://doi.org/10.3390/iot5030022

[50] A. Alsarhan, B. Igried, R. M. Bani Saleem, M. Alauthman, and M. Aljaidi, "Enhancing phishing URL detection: A comparative study of machine learning algorithms," in *Proceedings of the 2023*, 2023.

[51] M. Aljaidi, "Cybersecurity threats in the era of AI: Detection of phishing domains through classification rules," presented at the 2023 2nd International Engineering Conference on Electrical, Energy, and Artificial Intelligence (EICEEAI), Zarqa, Jordan, 2023.

[52] A. Almaini, A. Al-Dubai, I. Romdhani, M. Schramm, and A. Alsarhan, "Lightweight edge authentication for software defined networks," *Computing*, vol. 103, no. 2, pp. 291-311, 2021. https://doi.org/10.1007/s00607-020-00874-4

[53] Frost and Sullivan, "Automotive cybersecurity market, global, 2023–2030," Retrieved: https://store.frost.com/automotive-cybersecurity-market-global-2023-2030.html, 2025.

[54] K. KnowBe4, "KnowBe4, KnowBe4's 2022 phishing by industry benchmarking report reveals that 32.4% of untrained end users will fail a phishing Test," Retrieved: https://info.knowbe4.com/phishing-by-industry-benchmarking-report, 2022

[55] Kaspersky, "The rising threat of social engineering attacks. Kaspersky Lab Report," Retrieved: https://www.kaspersky.com. [Accessed 2021.

[56] M. Schöps, M. Gutfleisch, E. Wolter, and M. A. Sasse, "Simulated stress: A case study of the effects of a simulated phishing campaign on employees' perception, stress and self-efficacy," presented at the 33rd USENIX Security Symposium (USENIX Security 24), 2024.

[57] N. H. C. Kamaruddin and M. F. Zolkipli, "The role of multi-factor authentication in mitigating cyber threats," *Borneo International Journal*, vol. 7, no. 4, pp. 35-42, 2024. https://doi.org/10.13140/RG.2.2.15628.94083

[58] S. Harris, *CISSP all-in-one exam guide*. USA: McGraw-Hill Education, 2021.

[59] Y. E. Suzuki and S. A. S. Monroy, "Prevention and mitigation measures against phishing emails: A sequential schema model," *Secure of Journal*, vol. 35, pp. 1162–1182, 2022. https://doi.org/10.1057/s41284-021-00318-x

[60] C. T. Aghaunor, P. Eshua, T. Obah, and O. Aromokeye, "Data security strategies to avoid data breaches in modern information systems," *World Journal of Advanced Research and Reviews*, vol. 20, no. 3, pp. 251–258, 2025. https://doi.org/10.30574/wjarr.2023.20.3.2515

[61] M. Nacaroğlu, Ç. Tarhan, V. Tecim, and M. Komesli, "Cyber security based visitor control system design," *Journal of Information Systems and Management Research*, vol. 6, no. 1, pp. 13-25, 2024. https://doi.org/10.59940/jismar.1402494

[62] S. Sett and H. Gupta, "A biometric security model for the enhancement of data security," presented at the 2024 11th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO), IEEE, 2024.

[63] A. Ghadge, M. Weiß, N. D. Caldwell, and R. Wilding, "Managing cyber risk in supply chains: a review and research agenda," *Supply Chain Management: An International Journal*, vol. 25, no. 2, pp. 223-240, 2020. https://doi.org/10.1108/SCM-10-2018-0357

[64] A. Maraj and W. Butler, "Taxonomy of social engineering attacks: a survey of trends and future directions," presented at the The 17th International Conference on Cyber Warfare and Security, 2022.

[65] K. Mitnick and W. Simon, *The art of deception: Controlling the human element of security*. UK: Wiley, 2002.

[66] Y. Li, Z. Du, Y. Fu, and L. Liu, "Role-based access control model for inter-system cross-domain in multi-domain environment," *Applied Sciences*, vol. 12, no. 24, p. 13036, 2022. https://doi.org/10.3390/app122413036

[67] F. P. E. Putra, A. Zulfikri, G. Arifin, and R. M. Ilhamsyah, "Analysis of phishing attack trends, impacts and prevention methods: Literature study," *Brilliance: Research of Artificial Intelligence*, vol. 4, no. 1, pp. 413-421, 2024. https://doi.org/10.47709/brilliance.v4i1.4357

[68] B. S. Almutairi and A. Alghamdi, "The role of social engineering in cybersecurity and its impact," *Journal of Information Security*, vol. 13, no. 4, pp. 363-379, 2022. https://doi.org/10.4236/jis.2022.134020

[69] H. N. Fakhouri, B. Alhadidi, K. Omar, S. N. Makhadmeh, F. Hamad, and N. Z. Halalsheh, "Ai-driven solutions for social engineering attacks: Detection, prevention, and response," presented at the 2024 2nd International Conference on Cyber Resilience (ICCR), IEEE. , 2024.