The Journal of Technology Studies

# From Mitnick to Modern Database Threats: Evolution of Social Engineering Tactics and Their Impact on Data Integrity

APPLIED RESEARCH

NDUBUISI UKWADINACHI

VIRGINIA TECH PUBLISHING


## ABSTRACT

As technology continues to advance, database systems face growing threats from social engineering attacks that exploit human vulnerabilities. This work traces the evolution of social engineering methods, beginning with Kevin Mitnick's pioneering strategies and progressing to the highly sophisticated, AI-driven tactics used today. By examining major incidents of social engineering in recent years, this research highlights the significant impact these tactics have on data integrity and database security. It also evaluates modern social engineering techniques, including spear-phishing, vishing, and baiting, reverse social engineering, water-holing, quid pro quo, tailgating, and assesses the effectiveness of current mitigation techniques. Despite advancements in security measures, attackers continue to refine their approaches, exposing gaps in existing defenses. This work also explores a detailed list of possible directions to strengthen the resilience against these threats. It highlights the need for integrated cyber and database security strategies that combines technical and human safeguards to overcome future incidents. Overall, the work provides a roadmap for strengthening defenses and ensuring long-term resilience against social engineering attacks.



**CORRESPONDING AUTHOR:**
**Ndubuisi Ukwadinachi**
Epsilon Pi Tau, US
ndubuisi.uk@gmail.com



**KEYWORDS:**
Kevin Mitnick; Social Engineering; Database Integrity; Phishing; Vishing; Baiting; Reverse Social Engineering; Water-holing; Tailgating; Quid Pro Quo

**TO CITE THIS ARTICLE:**
Ukwadinachi, N. (2025). From Mitnick to Modern Database Threats: Evolution of Social Engineering Tactics and Their Impact on Data Integrity. *Journal of Technology Studies*, *50*(1), 14–29. DOI: https://doi.org/10.21061/jts.438

## 1. INTRODUCTION

The human aspect of computer security is frequently exploited and often neglected. Organizations invest millions in firewalls, encryption, and securing devices, but much of that effort is wasted if it doesn't address the most vulnerable link in the security chain: the people who use, manage, and operate the systems (Mitnick & Simon 2003). With rapid technological advancement, the database and cyber security landscape has become increasingly complex and as primary repositories for sensitive personal, financial, and operational data, databases have become prime targets for cyber attackers (Li, Zhou & Cao 2021). Among the most dangerous tactics used is social engineering, which manipulates human behavior to bypass even the most advanced technical safeguards. Social engineering is particularly strong because it exploits the weakest link in cyber security which is human nature (Falade 2023). Kevin Mitnick, one of the most iconic figures in the history of social engineering, revolutionized how attackers approach database infiltration in the late 20th century. Unlike most hackers of his time, who focused on exploiting software or hardware vulnerabilities, Mitnick understood that humans could be more easily manipulated than code (Wang et al. 2020). His techniques as shown in Figure 1, such as pretexting and dumpster diving, enabled unauthorized access to major organizations like Motorola and Sun Microsystems. Mitnick's legacy illustrates that, despite advancements in cyber security, humans remain a primary point of exploitation for adversaries, an insight that attackers continue to adapt today.

Kevin Mitnick's early social engineering tactics, once reliant on simple human manipulation, have evolved into complex strategies that now target entire data ecosystems, including networks, cloud systems, and databases. Today, attackers use Artificial Intelligence (AI) and machine learning to automate and personalize social engineering techniques, such as phishing and pretexting, allowing them to impersonate trusted figures and extract sensitive information with ease (Chetioui et al. 2022; Kathiravan et al. 2023). Social engineering methods like baiting and quid pro quo have also advanced, exploiting human psychological triggers like curiosity and urgency. AI-driven algorithms enhance the effectiveness of these tactics, making modern attacks more efficient, harder to detect, and increasingly damaging, often leading to ransomware deployment, organizational disruption, and financial loss (Becue, Praça & Gama 2021). As database systems have grown to store vast amounts of sensitive information, they have become high-value targets for cybercriminals, with human operators, administrators, and users representing potential entry points for social engineers (Aldawood & Skinner 2020). Attackers now use sophisticated methods, such as spear-phishing, to target specific individuals with customized messages designed to extract credentials or gain unauthorized access (Kwak et al. 2020). This level of precision far surpasses the generalized tactics of Mitnick's time. Modern attackers spend weeks or months researching their targets, creating believable narratives that significantly increase their chances of success.

Over the years, social engineering attackers have increasingly exploited human behavior to bypass

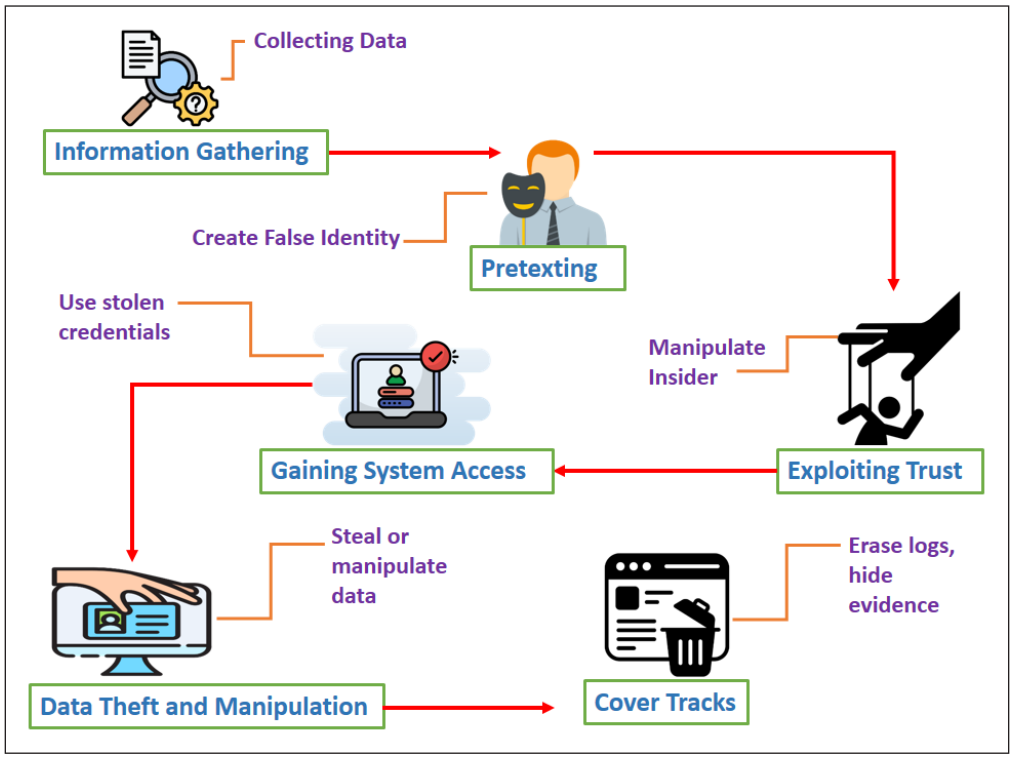


**Figure 1** Step-by-step process of Kevin Mitnick's social engineering attack.

advanced cybersecurity defenses. By leveraging psychological triggers like trust, authority, curiosity, and urgency, attackers have crafted increasingly sophisticated tactics to launch such attacks. As of 2023, social engineering attacks have reached a staggering 1.76 billion as shown in Figure 2 (Chheda 2024). One prominent example is the 2013 Target breach, where attackers phished a third-party vendor, leading to the theft of credit and debit cards from over 40 million customers, along with personal information from an additional 70 million customers. The breach resulted in an estimated financial loss of $292 million and Target faced severe reputational damage and legal challenges, including a $10 million class-action lawsuit settlement (Shu et al. 2017). In the 2016 Uber breach, attackers used vishing attack which is combination of voice and phishing to gain administrative credentials, exposing data of 57 million riders and drivers. The attackers accessed Uber's internal systems, exfiltrating data on 57 million riders and drivers (Kiesow Cortez 2020). Uber initially concealed the breach and paid $100,000 to the attackers to destroy the data, which led to severe legal consequences and eventual settlements amounting to $148 million in fines for failing to disclose the incident (Coffey 2019). Similarly, in 2020, Twitter was compromised through phone-based phishing, where attackers hijacked high-profile accounts to promote a crypto currency scam, resulting in reputational damage (Kekulluoglu, Magdy & Vaniea 2020). These incidents underscore the growing danger of social engineering, which continues to exploit human vulnerabilities, causing significant financial and reputational damage to organizations globally.

This paper examines how social engineering tactics have evolved in response to modern global threats, emphasizing how attackers exploit human vulnerabilities to compromise data integrity within a database infrastructure. Despite technical and human safeguards, social engineering remains the most effective method for bypassing robust defenses by obtaining sensitive information like passwords or exploiting insider cooperation. The research traces the evolution of social engineering techniques and offers insights into the existing approach employed to counter such attacks. Furthermore, this paper also highlights how organizations can better defend against these sophisticated attacks. It stresses the need for cyber and database security awareness and training and use of access control and authentication to prevent social engineering attacks. Ultimately, the paper connects the historical context with emerging security strategies, encouraging organizations to adapt their defenses to counter these persistent threats.

## 2. MODERN SOCIAL ENGINEERING TACTICS

As technology advances, so do the methods used by attackers to exploit human vulnerabilities. Modern social engineering tactics have evolved beyond basic deception due to integration of AI, machine learning (ML) and automation to bypass even the most robust security measures.

The integration of AI has now improved the way phishing and spear phishing tricked the victims. In past, it involved sending deceptive emails to trick individuals into revealing sensitive information. Now a days, with the use of AI, attackers employ context aware message using natural language processing and behavioral profiling to deceive the target and bypass spam filters (Jain & Gupta 2021). According to the FBI's 2023 Internet Crime Report, phishing remains the most frequently reported cybercrime, with losses amounting to over $44 million (Chan-Tin & Stalans 2023). The 2016 DNC breach, where attackers used spear-phishing to steal thousands of emails, is a notorious

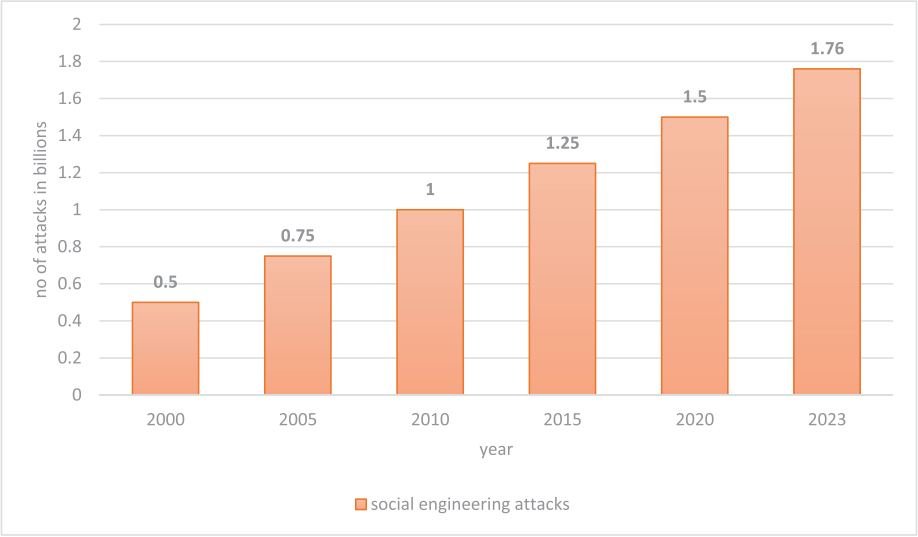


**Figure 2** Rise and prevalence of social engineering attacks (Chheda 2024).

example that demonstrates the potentially far-reaching consequences of these personalized attacks (Prevezianou 2021). There are different forms of social engineering attacks by researchers over the years as shown in Figure 3. Pretexting attacks are now more convincing than ever because of deep fake technologies which helps in the creation of a fabricated scenario (fake voice or fake video) designed to manipulate a target into revealing sensitive information or performing an action. Unlike phishing, which relies on creating a sense of urgency for quick decision-making, pretexting is more subtle, focusing on building trust over time (Mehta, Vora & Sachala 2021).

On the other hand, vishing relies on phone calls to impersonate legitimate entities, such as technical support or financial institutions, to extract confidential information. Now a days, the sophistication of these attacks are further improved by AI generated voices that can easy impersonate an organization executive or employees. Vishing attacks often result in the compromise of credentials, which can later be used to gain unauthorized access to sensitive databases or systems (Ashfaq et al. 2024). In baiting, attackers employ AI to integrate malware which is delivered through free software downloads or physical items like USB drives to bypass antivirus detection (Tulkarm 2021). One real-world example is from 2008, when attackers left infected USB drives in the parking lot of the US base. Curious employees plugged the devices into their work computers, unknowingly installing malware that allowed attackers to gain unauthorized access to sensitive defense systems. This breach led to increased scrutiny on physical security protocols across defense contractors (Roberts 2010).

Water holing attacks have not evolved into more targeted attacks with AI algorithm identifying which websites target groups should visit to inject a malicious code or malware (Ismail et al. 2017). In 2019, cybercriminals injected malicious code into legitimate websites frequented by individuals and organizations related to religious, charity, and volunteer sectors. Visitors to these compromised sites were unknowingly subjected to a drive-by download, where malware was silently installed on their devices without their knowledge (Paganini 2020). Furthermore, the quid pro quo attacks, where attackers offer services or benefits in exchange for sensitive information, are now carried out by AI based chat-bots posing as tech support in real time chat interfaces (Kamruzzaman et al. 2023). In 2018, an attacker posed as tech support for Arizona-based Banner Health, convincing employees to provide login credentials under the guise of system upgrades. The breach cost the company millions in compliance fines and forced significant operational changes (John, Ravichandran & Khan 2018).

Reverse social engineering involves deliberately creating a problem, after which the attacker poses as a solution provider to gain victim trust (Krombholz et al. 2015). Now a days, the attackers employ spoofed system errors and automated alerts generators to lure the victim into making contact. Even physical attacks like tailgating are harder to detect because they integrate behavioral profiling with physical deception to gain physical access to a restricted area.

These advancements indicate that social engineering has moved from traditional manual manipulation to more sophisticated, coordinated and data driven methods empowered by AI and ML. As attackers shift their methods towards automated behavioral profiling

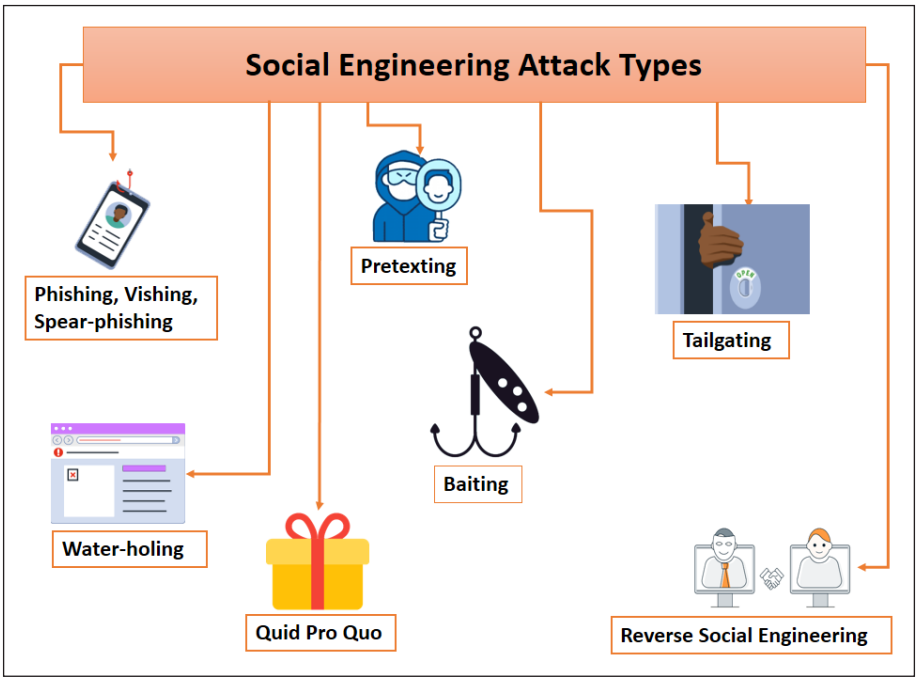


**Figure 3** Different forms of social engineering attacks.

and exploit decision making biases, traditional methods for awareness and training to counter such attacks need to be supplemented with advanced behavior awareness systems and technical countermeasures.

## 3. SOCIAL ENGINEERING ATTACKS IMPACT ON DATABASE INTEGRITY

Social engineering attacks pose a significant threat to database integrity by exploiting the human element in organizational security frameworks. These attacks manipulate individuals into revealing sensitive information, such as login credentials to bypass authentication measures. Once attackers gain unauthorized access, they can manipulate, delete, or insert false data, compromising the accuracy and reliability of the database (Soni & Mathew 2020). This differs from traditional hacking, which exploits technical flaws, as social engineering undermines the trust users place in legitimate processes, making it harder to detect and prevent. For example, phishing attacks may lure employees into revealing passwords or downloading malicious software that allows attackers to alter database entries undetected. These manipulations can result in incorrect financial records, falsified personal information, or changes in access privileges leading to significant disruptions in data-driven decision-making (Jakala & Pekkola 2007). In the context of enterprise databases, social engineering attacks can have a cascading impact affecting not just the targeted system but also interconnected platforms and services reliant on accurate data. Once compromised, database integrity becomes a challenge to restore, often requiring detailed forensic analysis to uncover the extent of the manipulation. Organizations may face operational setbacks, loss of reputation, legal penalties, and diminished customer trust, especially if the attack goes undetected for an extended period (Neto et al. 2021). In this section, we explore different case studies of known social engineering attacks, their consequences and also explore the consequences of database integrity compromise.

### 3.1 CASE STUDIES OF NOTABLE BREACHES AND THEIR CONSEQUENCES

- **Sony Pictures Hack (2014):** Attackers used phishing to lure Sony employees into revealing their credentials, which allowed the attackers to infiltrate the corporate network. They then exfiltrated sensitive emails, internal documents, and unreleased films while erasing key data from Sony's servers. Although the primary objective was not to alter the integrity of Sony's databases, the incident underscored the broader risks social engineering presents to data integrity. Figure 4 indicates the impact of Sony pictures breach on its revenue (Haggard & Lindsay 2015; Sicard 2015; Quader & Janeja 2021).
- **The Snowden Revelations (2013):** Snowden, a contractor for the National Security Agency (NSA), used social engineering to persuade colleagues to reveal their login credentials. Armed with these credentials, he accessed and exfiltrated vast amounts of classified data (Boussios 2021). The case revealed how trusted insiders, leveraging social engineering, could become significant threats to database integrity.
- **Toyota Boshoku:** Attackers defrauded Toyota Boshoku Corporation of $37 million through a business email compromise (BEC) scam by persuading a finance executive to redirect wire transfers to falsified account details (Gatefy). The case demonstrates how attackers can manipulate

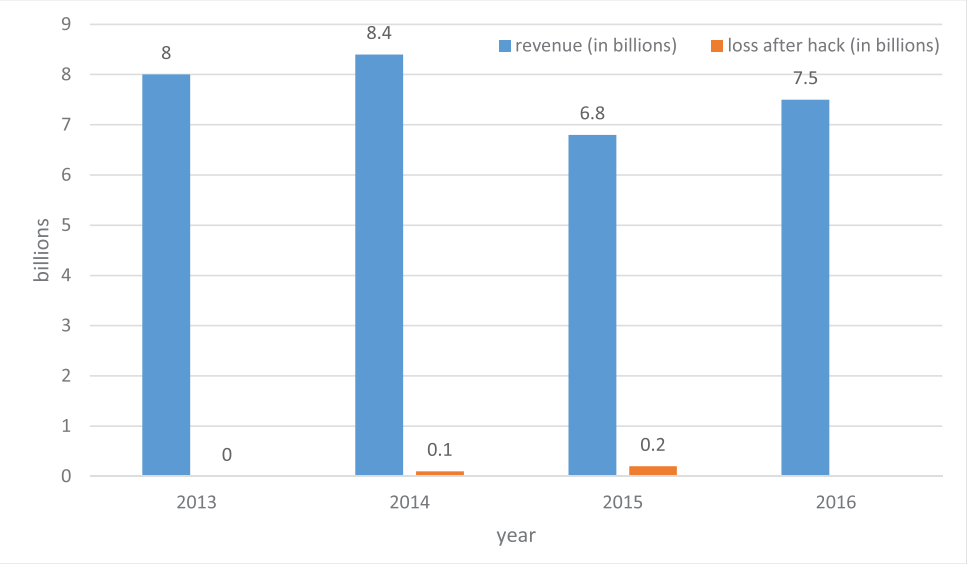


**Figure 4** Statistics of Sony picture revenue before and after 2014 hack.

data, including database records tied to financial transactions.

- **OCBC Bank Phishing Scam (2021):** This case involved the Oversea-Chinese Banking Corporation (OCBC), where phishing attacks led to the loss of $8.5 million from 470 customers. Attackers created fraudulent websites mimicking the bank's interface, tricking users into revealing login credentials. Figure 5 highlights the impact of OCBC Bank Phishing Scam.
- **Colonial Pipeline Attack:** A ransomware attack enabled through social engineering tactics resulted in shutdown of fuel supply across the East Coast. The company reportedly paid approximately $4.4 million in ransom to regain control of its systems (Beerman et al. 2023; Pitman & Crosier 2024).

These cases highlight how social engineering attacks, particularly those targeting human errors, can lead to data compromise in a database system. By gaining unauthorized access, attackers can alter or delete key records, impacting data accuracy and trust. Companies facing such attacks must deal not only with the immediate financial and reputational damage but also with long-term challenges in restoring database integrity.

## 3.2 CONSEQUENCES OF DATABASE INTEGRITY COMPROMISE

The consequences of social engineering attacks on database integrity are severe and multifaceted, impacting organizations across various dimensions, including operational efficiency, legal liabilities, financial stability, and overall reputation as depicted in Figure 6. Importantly, these breaches also raise significant concerns related to national security, particularly when sensitive governmental or critical infrastructure data is compromised.

### 3.2.1 Operational disruption

When data is corrupted or manipulated, organizations struggle to maintain normal business functions. In critical sectors such as healthcare, an erroneous database could lead to misdiagnoses or improper patient care. For national security, disruptions in critical infrastructure such as energy, transportation, and emergency services can have devastating effects on public safety and security (Orlando 2021; Patrick, Brett van Niekerk & Fields 2019).

### 3.2.2 Legal and financial repercussions

Data integrity breaches expose organizations to significant legal challenges, and they may face lawsuits from affected individuals or businesses, especially if personal information is altered, compromised, or lost. For example, under GDPR, organizations can face fines of up to €20 million or 4% of their global annual turnover for failing to protect personal data (Başak Erdogan 2021; Hoofnagle, Sloot & Borgesius 2019; Presthus & Sonslien 2021).

### 3.2.3 Reputation damage

The fallout from a data breach often includes severe damage to an organization's reputation. Once a breach is publicized, customer trust can erode quickly, as stakeholders question the organization's commitment to safeguarding sensitive information. A good example is the 2017 Equifax breach, which exposed the personal data of approximately 147 million individuals, resulting in a significant reputational harm, with many customers choosing to sever ties with the company (Perera et al. 2022; Novak & Vilceanu 2019).


**Figure 5** Impact of OCBC Bank phishing scam.

### 3.2.4 Difficulty in restoring data

The process of restoring database integrity following a breach is typically complex and resource-intensive. Organizations often engage forensic experts to conduct thorough investigations, assess the extent of the damage, and determine the vulnerabilities that allowed the breach to occur (Bansal 2019). In sectors related to national security, such as intelligence or defense, even minor inaccuracies in data can lead to grave consequences, potentially jeopardizing national interests or security operations. The time taken to restore integrity can lead to prolonged operational setbacks, impacting response times in critical situations (Hathaway & Klimburg 2012).

### 3.2.5 Erosion of competitive advantage

A compromised database can diminish an organization's competitive advantage in the marketplace, especially for companies engaged in national security or defense contracts. Businesses known for their commitment to data security may find their reputations tarnished by breaches, leading competitors to capitalize on their vulnerabilities. The loss of contracts with governmental bodies can have cascading effects, affecting not just the organization but also the national supply chain for critical goods and services (Morse, Raval & Wingender 2011).

### 3.2.6 Increased security costs

Following a data breach, organizations often face heightened security costs as they scramble to bolster their defenses against future attacks. This may involve hiring additional data security experts, investing in advanced security technologies, and conducting regular security audits. For organizations linked to national security, the stakes are even higher, as failures in cybersecurity can lead to threats against public safety (Algarni & Malaiya 2016).

### 3.2.7 National security implications

When social engineering attacks target organizations that handle sensitive governmental or critical database infrastructure, the implications extend to national security. Compromised databases may contain data intelligence, defense strategies, or infrastructure plans vital to national interests. For instance, a successful breach at a defense contractor could provide adversaries with insight into military operations, potentially undermining national defense (Smith & Mulrain 2017).

### 3.3 AI DRIVEN ESCALATION

The increasing advancement in AI and ML allows attackers to scale social engineering attacks without putting in a huge effort. Nowadays, AI-based algorithms can generate phishing emails, generate fake speech patterns to mimic voice, and detect suitable targets through data mining. This type of automation not only reduces the labor cost but also enhances the success ratio, making data integrity more vulnerable than ever.

Organizations should shift their focus towards both the technical safety measures and human awareness. As attackers are armed with new capabilities due to AI, cyber detection and mitigation methods should employ behavior-based detection, role-based access controls, and real-time monitoring to detect suspicious activities in real-time

## 4. METHODOLOGY

This section outlines the research methods and systematic approach used to conduct the work on the evolution of social engineering tactics and their impact. The goal is to distinguish the patterns and assess how

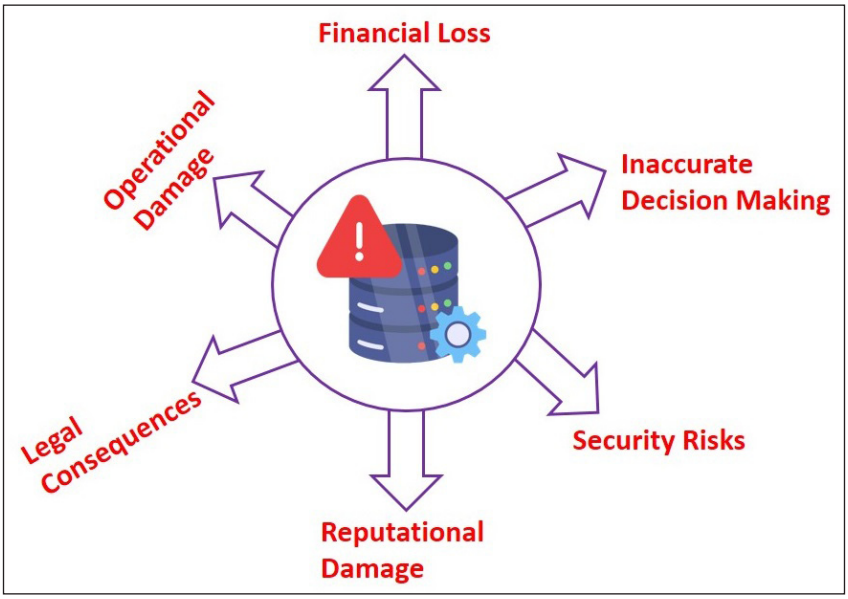


**Figure 6** Consequences of database integrity loss.

modern technologies such as artificial intelligence (AI) and machine learning (ML) have improved the efficiency of social engineering attacks.

## 4.1 RESEARCH DESIGN

The research was designed as a qualitative survey**,** aiming to synthesize existing studies, case reports, and data on social engineering tactics in database/cybersecurity. The goal was to trace the development of social engineering strategies over time and assess their implications for modern database systems. A systematic review approach ensured inclusion of the most relevant and high-quality sources by categorizing different attacks, their outcomes, and techniques employed, which were documented in the reviewed sources.

## 4.2 DATA COLLECTION

Data collection involved a thorough search of peer-reviewed academic journals**,** industry reports**,** and reputable cybersecurity white papers**.** The following databases were accessed:

- IEEE Xplore
- Google Scholar
- ScienceDirect
- ACM Digital Library
- Others

Relevant reports from cybersecurity organizations, reputable sources, and media coverage of breaches were also incorporated. Keywords used in the research included:

- 'Social engineering tactics'
- 'Cybersecurity threats'
- 'Database security'
- 'Phishing, vishing, spear-phishing'
- 'Kevin Mitnick social engineering'
- 'AI-driven social engineering'

## 4.3 INCLUSION CRITERIA

To ensure relevance and correctness, the following inclusion criteria was used.

- **Time Frame:** Studies and reports from the last two decades (2000–2023) were included.
- **Content:** Particular emphasis on those involving real-world case studies, technical analysis of breaches, and advancements in mitigation techniques.
- **Relevance:** Incidents must show an indirect or direct impact on database integrity (such as unauthorized access, data manipulation).
- **Documentation:** Focus on those public or scholarly documents which highlights the impact and scope of the breaches.
- **Technology Used:** Special preference was given to modern methods employing AI.

### 4.3.1 Application of inclusion criteria

*A three-step screening process was applied to apply the inclusion criteria.*

- **Preliminary Screening:** Titles and abstracts were reviewed to exclude studies that are irrelevant and overly technical and do not involve social engineering or database breaches.
- **Full Text Review:** The selected papers were reviewed in full to ensure the availability of all five criteria, especially focusing on documentation quality and its coherence with data integrity.
- **Comparative Assessment:** The selected case studies were then compared on the basis of through details information they offer, the attack sophistication, and the presence of technological integration. Studies that highly met this criterion were then considered for final analysis.

## 4.4 DATA ANALYSIS

The data analysis was conducted through content analysis to identify key themes, such as the evolution of tactics from traditional social engineering to AI-driven methods. The thematic analysis focused on:

- Classification of social engineering tactics (e.g., phishing, spear-phishing, pretexting).
- The relationship between social engineering tactics and database integrity**.**
- The effectiveness of mitigation strategies**,** including technical and human-centered approaches.
- Each study and case report were examined for patterns in how attackers exploit human vulnerabilities and how these have evolved over time. This was further connected to how breaches impact database integrity, with emphasis on data manipulation and unauthorized access.

## 4.5 CASE STUDY SELECTION

A purposive sampling method was used to select case studies that exemplify the broader trends in social engineering attacks. These case studies were chosen based on:

- The use of advanced or novel social engineering techniques.
- Impact on data integrity, organizational operations and national security.
- Availability of detailed incident information.
- Inclusion of various sectors (finance, healthcare, government, energy)

Selected case studies were analyzed in depth to extract common social engineering strategies and their implications for cyber security.

### 4.6 VALIDATION OF FINDINGS

To ensure the reliability of the findings, a triangulation method was employed. Information from academic sources**,** real-world case studies, and industry reports was cross-referenced to verify consistency and accuracy. This method helped minimize bias and provided a comprehensive view of the evolution of social engineering tactics.

## 5. EXISTING TECHNIQUE TO MITIGATE SOCIAL ENGINEERING ATTACKS

Social engineering attacks exploit human psychology, making them one of the most challenging forms of cyber threats to defend against. As these attacks increasingly target organizations' most vulnerable asset people various strategies have been developed to mitigate their impact. Butt et al. (2022) proposed a system to detect phishing emails using machine learning and deep learning models, specifically Support Vector Machine (VM), Naive Bayes (NB), and LSTM. They created a dataset with legitimate and phishing emails, applied feature extraction techniques, and trained the models for classification. Their approach achieved high accuracy rates, with SVM reaching 99.62%, NB 97%, and LSTM 98%. They suggested improving the system by combining phishing and legitimate emails into a more dynamic dataset to better reflect real-world conditions. The proposed framework aims to enhance protection against evolving phishing attacks across organizations. Another technique to detect phishing attack was proposed by (Salahdine, El Mrabet & Kaabouch 2021), in which they utilized machine learning-based technique for detecting phishing attacks, focusing on emails. They collected and analyzed over 4000 phishing emails and built a dataset with 10 relevant features. The dataset was used to train, validate, and test three classifiers: Support Vector Machine (SVM), Logistic Regression (LR), and Artificial Neural Network (ANN). Through parametric studies, they found that SVM, LR, and ANN achieved high accuracy, with the ANN model performing best using two hidden layers and the Relu activation function. This model offers fast and accurate phishing detection. Benavides-Astudillo et al. (2023) proposed a phishing detection model that focuses on analyzing the text of suspicious web pages, rather than just URLs, using Natural Language Processing (NLP), and Deep Learning (DL) algorithms. They applied the Keras Embedding Layer with GloVe to capture semantic and syntactic features of web page content and tested four DL algorithms: LSTM, BiLSTM, GRU, and BiGRU. Their experiments showed that BiGRU performed the best, achieving a mean accuracy of 97.39%. The study highlights the potential of using word embeddings and DL algorithms for effective phishing detection.

To deal with sub type of phishing attack called vishing, Fakieh & Akremi (2022) proposed blockchain technology-based mechanism to enhance security. Their model is based on two key principles: dual control (requiring more than one entity to complete a task) and split knowledge (dividing critical information between entities). By incorporating blockchain, the model ensures secure, transparent, and immutable records of transactions, reducing reliance on human vulnerability. The paper highlights its effectiveness in handling vishing attacks and demonstrates how the model can be easily adopted by organizations using open-source blockchain platforms. Al-Hamar et al. (2021) put forward a solution to detect spear-phishing attacks by analyzing domain authenticity, which attackers often manipulate to gain trust. Their detection system uses multiple algorithms to evaluate whether a domain is genuine or fraudulent, significantly improving phishing detection. Tests conducted showed it outperformed existing email security systems, in identifying spear-phishing and whaling attacks. Through real-world testing, their work successfully detected phishing emails that other systems failed to recognize, demonstrating its potential to enhance protection against enterprise-targeted attacks. Sonowal et al. (2021) took an approach to handle traditional phishing and spear-phishing emails using multi-dimensional features such as domain validation, writing style, and an auto-upgrade profile is proposed. The method employs a machine-learning algorithm to classify phishing emails and includes an additional layer of security through a verifiable secret-sharing scheme to authenticate email senders. This approach effectively enhances the detection of phishing attacks by leveraging various features and adding a unique verification step.

Researchers have also worked over the years to handle watering hole attacks. Allen et al. (2020) proposes Mnemosyne, a forensic analysis engine designed to investigate watering hole attacks, where attackers compromise a frequently visited website to infiltrate an organization's network. Mnemosyne passively collects browser activity logs to detect when and how a website was compromised. It then traces the impact of the attack on specific users within the targeted enterprise. Through real-world tests, the system effectively identified victims and reduced manual analysis effort by over 98%. Mnemosyne enhances post-attack investigations, pinpointing the attack timeline and affected employees. Irani et al. (2011) examine reverse social engineering (RSE) attacks within social networks, where the victim initiates contact with the attacker, establishing trust. Unlike traditional social engineering, RSE manipulates features like friend recommendations, visitor tracking, and

demographic-based searches to lure users. Their work discusses three novel RSE attack strategies, demonstrating their effectiveness in real-world scenarios. Their work also shows that attackers can attract victims without sending friend requests, simply by creating enticing profiles. The study highlights the need for social networks to implement countermeasures against RSE threats.

Tailgating attack, which is a form of social engineering attack, poses significant threat to physical security. To handle this, Akati & Conrad (2021) proposed a three-step anti-tailgating solution to address the shortcomings of existing security technologies. This system combines face detection, palm recognition, and motion sensors to detect multiple individuals or fast-paced entries that bypass single access authorizations. The design science methodology and experimental approaches were used to develop and test this solution. Results demonstrated that the combination of these technologies effectively prevents tailgating by overcoming limitations of prior methods. This system significantly enhances security for organizations**.** Girinoto et al. (2022) explored how phishing attacks could be executed by pretexting within the OmeTV video chat application, targeting users from Indonesia over 18. They proposed a Social Engineering Session (SES) attack methodology to extract personal information from victims by building trust. The results showed that the attack successfully gathered sensitive details, such as full name, date of birth, address, hobbies,

| EXISTING TECHNIQUE | TYPE OF ATTACK | METHOD USED | ADVANTAGE | LIMITATION |
|---|---|---|---|---|
| **Butt et al. (2022)** | Phishing (Email) | Machine Learning and Deep Learning models | Improvement in mitigation by combining dynamic phishing and legitimate emails. | 1. Relying solely on pre-defined features<br>2. It limits the model's adaptability |
| **Salahdine et al. (2021)** | Phishing (Email) | Machine Learning based models | Achieved high accuracy in phishing detection. | Attackers can manipulate search engine rankings to make malicious webpages appear legitimate, reducing the effectiveness of heuristic-based method. |
| **Benavides-Astudillo et al. (2023)** | Phishing (Webpage) | NLP and Deep Learning | BiGRU model achieved the best results with a mean accuracy of 97.39%. | Explores web page text rather than URLs, phishing attacks often manipulate URLs in deceptive ways |
| **Fakieh & Akremi (2022)** | Vishing | Blockchain based mechanism | Secure, transparent, and immutable records to enhance security, effective for vishing attacks. | Lack of ability to address more complex social engineering attacks that use multiple vectors like phishing, smishing, or in-person manipulation. |
| **Al-Hamar et al. (2021)** | Spear-phishing (Email) | Domain authenticity analysis | Outperformed existing email security systems in detecting spear-phishing and whaling attacks. | It may not be effective against phishing attacks using compromised legitimate domains or non-domain-based tactics. |
| **Sonowal et al. (2021)** | Phishing (Email) | Multi-dimensional feature analysis | Enhanced detection using multiple features and an additional verification layer. | Use of whitelist-based profile for spear-phishing detection may limit its effectiveness against targeted attacks that exploit familiar contacts. |
| **Allen et al. (2020)** | Water-holing | Forensic analysis engine (Mnemosyne | Reduced manual analysis effort by 98%, enhanced post-attack investigation. | Limited visibility when investigating attacks that rely on a drive by download. |
| **Irani et al. (2011)** | Reverse social engineering | Analysis of social networks feature | Demonstrated novel RSE attack strategies and their effectiveness, highlighting the need for countermeasures on social networks. | Overlook contextual factors, such as variations in user behavior, platform policies, and the evolving nature of social engineering tactics. |
| **Akati & Conrad (2021)** | Tail-gaiting | Anti-tailgating solution | Effective prevention of tailgating by overcoming limitations of prior methods. | Lacks full physical implementation and practical testing, confining it to theoretical design and minimal software experimentation. |
| **Girinoto et al. (2022)** | Pretexting | Social Engineering Session (SES) attack methodology | Successfully gathered sensitive information using pretexting, demonstrating the potential for fraud or marketing exploitation. | Does not account for the broader applicability of the findings across different user groups or platforms. |

**Table 1** Comparison of existing techniques used for mitigation of social engineering attacks.

Instagram account, and phone number. They also suggested that this information could be further exploited for fraud or marketing purposes. The study highlights the effectiveness of pretexting in phishing attacks. A detailed comparison of state-of-the-art method used for social engineering attacks are shown in Table 1.

### 5.1 LIMITATION

Despite the significant progress made by researchers in addressing phishing attacks through machine learning, behavioral analytics, and other advanced detection methods, there remains a critical gap in the exploration of other social engineering tactics. Techniques, like baiting and Quid Pro Quo, which exploit curiosity and human psychology have not been as thoroughly investigated. Furthermore, reverse social engineering, pretexting, water-holing, and tailgating have not received the same level of attention and there are limited approaches and few concrete strategies or tools exist to mitigate these methods, leaving organizations vulnerable to these underexplored threats. More research is needed to develop comprehensive defense mechanisms that can detect and prevent these forms of social engineering, ensuring a more effective approach to handling such attacks.

## 6. MEASURES TO PROTECT FROM SOCIAL ENGINEERING ATTACKS

Organizations must educate and provide training to their employees on recognizing and responding to social engineering tactics, as human awareness remains the first line of defense. Regular cyber security awareness programs can help staff identify phishing, pretexting, baiting, and other deceptive schemes that exploit human behavior. In addition to education, organizations should implement multi-layered security protocols, such as two-factor authentication and strict access controls, to reduce the chances of successful attacks. Continuous monitoring, alongside incident response simulations, can also prepare employees to act swiftly in case of a breach. A comprehensive approach that combines education, technological safeguards, and policy enforcement is critical to mitigating the growing threat of social engineering attacks.

In their work, Weaver et al. (2021) emphasized that effective training should guide users on specific elements to look for when determining if an email is phishing. These cues include scrutinizing the sender's email address to ensure it matches the legitimate domain of the organization, checking for subtle discrepancies in the URL of links by hovering over them to preview the actual destination, and watching for common red flags like urgent or threatening language aimed at creating a sense of panic. Users were also trained to identify unusual requests for personal or financial information, especially in unsolicited emails. Additionally, they were encouraged to look for inconsistencies in the email format, spelling or grammar errors, and unfamiliar logos or poor-quality images. By teaching users how to verify these indicators, the training helped them more confidently classify emails as phishing or legitimate, even when phishing emails appeared highly sophisticated. The study conducted by Thomas (2018) emphasized the importance of personalized training tailored to different user groups to improve phishing detection and enhance overall security awareness within organizations. The author proposed a method to identify phishing attacks by conducting interviews with seven security experts. The authors conducted interviews with seven security experts to explore methods for empowering users to resist phishing attacks. They identified nine key themes that help distinguish users who are vulnerable to phishing from those who are more resilient. These themes include awareness of cybersecurity threats, email analysis skills, caution with unsolicited communications, trust in organizational policies, personal experience with phishing, technical proficiency, confidence in judgment, frequency of training, and responsiveness to authority. By addressing these factors, organizations can enhance phishing detection and improve overall cybersecurity awareness, reducing the likelihood of successful attacks.

According to Salahdine & Kaabouch (2019), to prevent tailgating attacks, awareness programs and training should be introduced on the importance of not allowing unauthorized individuals to follow them into secure areas, even out of politeness. Training should emphasize strict adherence to access protocols, such as ensuring each person uses their own credentials and reporting suspicious behavior. Employees can also be taught to challenge unknown individuals or direct them to security personnel. Regular awareness campaigns and physical security drills can reinforce this behavior. Training should highlight real-life examples of tailgating incidents and their consequences.

Vadrevu & Perdisci (2019) discusses that flow whitelisting is a proactive security measure that can effectively prevent social engineering attacks if employed by organizations. By restricting the actions and access of users within a system and by defining a set of trusted actions and entities, it limits unauthorized interactions that attackers might exploit. This approach reduces the attack surface, making it more difficult for social engineers to execute their attack. Additionally, monitoring user behavior against established patterns can help identify suspicious activities, triggering alerts for potential threats.

According to Montanez et al. (2022), access control is crucial in minimizing social engineering attacks by

limiting who can access sensitive information and systems. By implementing role-based access controls (RBAC), organizations can ensure that employees only have access to the information necessary for their specific job functions. This reduces the chances of an attacker obtaining sensitive data through manipulation or deception. Additionally, Siadati et al. (2017) states enforcing multi-factor authentication adds another layer of security, making it more difficult for unauthorized individuals to gain access, even if they manage to deceive an employee into revealing their credentials. Overall, robust access control measures help create barriers that protect against exploitation by social engineers. Table 2 provides a deep insight into measures employed against social engineering attacks.

## 7. FUTURE DIRECTIONS

As social engineering attacks are continuously evolving, social engineering attackers are exploiting human psychology, system vulnerabilities, and advanced technologies to launch more sophisticated and targeted attacks. It is necessary that future work should focus on the following directions to handle the increasing threats to database integrity.

- In the future, researchers should employ machine learning methods for the detection and mitigation of anomalies that indicate social engineering attacks. Natural language processing (NLP) can also be incorporated into voice recognition systems and email filters to detect suspicious activities, in particular phishing and vishing attempts.
- Conventional access control systems fail against credential-based attacks. Future work should use decentralized identity systems and continuous authentication methods that employ biometrics and behavioral patterns. This will help minimize the damage even when credentials are compromised through social engineering.
- With the advancement in AI, attackers generate fake media in pretexting and impersonation. To overcome that, researchers should design plug-and-play verification tools that are able to integrate with organizations' video conferencing, email, and HR systems to detect manipulated content.
- The human remains the most vulnerable element. Future research should integrate cognitive behavioral insights into training programs, transforming awareness into behavioral resistance.
- Social engineering attacks also take advantage of interconnected systems across different sectors. In the future, policy and infrastructure should provide robust, anonymized sharing of threat data between organizations to improve the defense against evolving social emerging methods.
- In the majority of cases, the breaches remain poorly documented or underreported. Future researchers

| MEASURE | SOURCE | BENEFITS | CHALLENGES | RECOMMENDATIONS |
|---|---|---|---|---|
| Employee Education & Training | Weaver et al. (2021); Thomas (2018) | Increases awareness and ability to identify threats. | Time and resources required for effective training. | Schedule regular training sessions and updates. |
| Multi-layered Security Protocols | Montanez et al. (2022); Siadati et al. (2017) | Reduces risk of unauthorized access. | Complexity can lead to user frustration or non-compliance. | Regularly review and update protocols for effectiveness. |
| Continuous Monitoring | Vadrevu & Perdisci (2019) | Early detection of potential threats. | Requires robust infrastructure and resources | Invest in monitoring tools and regular audits. |
| Phishing Detection Training | Weaver et al. (2021) | Empowers users to make informed decisions. | Users may still fall for sophisticated attacks. | Use real-life examples to illustrate threats effectively. |
| Tailgating Prevention | Salahdine & Kaabouch (2019) | Enhances physical security and reduces risk of breaches. | Difficult to enforce consistent behavior. | Conduct regular drills and emphasize the importance of vigilance. |
| Flow Whitelisting | Vadrevu & Perdisci (2019) | Reduces attack surface and improves overall security. | can be challenging to maintain an updated whitelist. | Regularly review and adjust whitelists based on new threats. |
| Access Control | Montanez et al. (2022) | Minimizes potential damage from insider threats | Complexity in managing access rights can arise. | Regular audits to ensure appropriate access levels. |
| Multi-factor Authentication | Siadati et al. (2017) | Significantly increases security against credential theft. | Users may resist additional steps in the login process | Educate users on the importance and benefits of multi factor authentication. |

**Table 2** Social Engineering attacks protective measures.

should focus on the development of standardized breach taxonomies that not only classify the technical vectors but also the components of social engineering. Such work will help improve public awareness and large-scale analysis.

## 8. CONCLUSION

Kevin Mitnick's pioneering social engineering tactics revealed the profound vulnerability of human nature in cyber security. Since then, attackers have significantly advanced their strategies, blending psychological manipulation with sophisticated technologies to target database integrity with increasing precision. In this study, we have explored in depth various types of social engineering attacks, illustrating their impact through real-world examples. Furthermore, we examined existing techniques, including machine learning-based detection systems and block chain, for securing access alongside preventive measures that individuals and organizations should adopt to mitigate the risks posed by social engineers. We also highlighted the limitations of these existing approaches and explored potential future directions that should be employed to handle the ever-evolving threat of social engineering attacks. Ultimately, this study highlights the critical need for comprehensive and adaptive defenses, combining technology, human awareness, and continuous innovation to safeguard databases and prevent future breaches.

## DATA ACCESSIBILITY STATEMENT

The data analysed in this study is taken from publicly available academic sources, industry reports, white papers, and documented cases of incidents and breaches. A full list of sources is included in the references. Detailed indexing criteria and source material are available upon request.

## FUNDING INFORMATION

This research received no external funding.

## COMPETING INTERESTS

The author has no competing interests to declare.

## AUTHOR AFFILIATIONS

**Ndubuisi Ukwadinachi** orcid.org/0009-0006-2797-507X
Epsilon Pi Tau, US

## REFERENCES

**Akati, J.,** & **Conrad, M.** (2021, October). Anti-tailgating solution using biometric authentication, motion sensors and image recognition. *2021 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress*, 825–830. DOI: https://doi.org/10.1109/DASC-PICom-CBDCom-CyberSciTech52372.2021.00137

**Aldawood, H.,** & **Skinner, G.** (2020). Analysis and findings of social engineering industry experts explorative interviews: Perspectives on measures, tools, and solutions. *IEEE Access*, *8*, 67321–67329. DOI: https://doi.org/10.1109/access.2020.2983280

**Algarni, A. M.,** & **Malaiya, Y. K.** (2016). A consolidated approach for estimation of data security breach costs. *2016 2nd International Conference on Information Management (ICIM)*, 26–39. DOI: https://doi.org/10.1109/infoman.2016.7477530

**Al-Hamar, Y., Kolivand, H., Tajdini, M., Saba, T.,** & **Ramachandran, V.** (2021). Enterprise credential spear-phishing attack detection. *Computers & Electrical Engineering*, *94*, 107363. DOI: https://doi.org/10.1016/j.compeleceng.2021.107363

**Allen, J., Yang, Z., Landen, M., Bhat, R., Grover, H., Chang, A., Ji, Y., Perdisci, R.,** & **Lee, W.** (2020). Mnemosyne: An effective and efficient postmortem watering hole attack investigation system. *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, 787–802. DOI: https://doi.org/10.1145/3372297.3423355

**Ashfaq, S., Chandre, P., Pathan, S., Mande, U., Nimbalkar, M.,** & **Mahalle, P.** (2024). Defending against vishing attacks: A comprehensive review for prevention and mitigation techniques. *Lecture Notes in Networks and Systems*, *896*, 411–422. DOI: https://doi.org/10.1007/978-981-99-9811-1_33

**Bansal, M., Grover, D.,** & **Sharma, D.** (2019). Storage and query over encrypted sensitive association rules in database. *International Journal of Internet Technology and Secured Transactions*, *9*(3), 242–259. DOI: https://doi.org/10.1504/IJITST.2019.101818

**Becue, A., Praça, I.,** & **Gama, J.** (2021). Artificial intelligence, cyber-threats and Industry 4.0: challenges and opportunities. *Artificial Intelligence Review*, *54*. DOI: https://doi.org/10.1007/s10462-020-09942-2

**Beerman, J., Berent, D., Falter, Z.,** & **Bhunia, S.** (2023, May). A review of colonial pipeline ransomware attack. *2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops*, 8–15. DOI: https://doi.org/10.1109/CCGridW59191.2023.00017

**Benavides-Astudillo, E., Fuertes, W., Sanchez-Gordon, S., Nuñez-Agurto, D.,** & **Rodríguez-Galán, G.** (2023). A phishing-attack-detection model using natural language processing and deep learning. *Applied Sciences*, *13*(9), 5275. DOI: https://doi.org/10.3390/app13095275

**Boussios, E.** (2021). Because of Snowden? The three leakers and privacy issues in the cyber matrix. *Research and Innovation Forum, 2021*, 513–528. Springer International Publishing. DOI: https://doi.org/10.1007/978-3-030-84311-3_47

**Butt, U. A., Amin, R., Aldabbas, H., Mohan, S., Alouffi, B.,** & **Ahmadian, A.** (2022). Cloud-based email phishing attack using machine and deep learning algorithm. *Complex & Intelligent Systems*, *9*, 3043–3070. DOI: https://doi.org/10.1007/s40747-022-00760-3

**Chan-Tin, E.,** & **Stalans, L. J.** (2023). *Phishing for profit*. Edward Elgar Publishing EBooks (pp. 54–71). DOI: https://doi.org/10.4337/9781800886643.00011

**Chetioui, K., Bah, B., Alami, A. O.,** & **Bahnasse, A.** (2022). Overview of social engineering attacks on social networks. *Procedia Computer Science*, *198*(1877–0509), 656–661. DOI: https://doi.org/10.1016/j.procs.2021.12.302

**Chheda, H.** (2024, July 29). *75+ Social engineering statistics for 2024*. Sprinto. https://sprinto.com/blog/social-engineering-statistics/

**Coffey, J. W.** (2019). Difficulties in determining data breach impacts. *Systemics, Cybernetics and Informatics, 17*(5).

**Erdoğan, B.** (2021). Data protection around the world: Turkey. In E. Kiesow Cortez (Ed.), *Data protection around the world: Privacy laws in action* (pp. 203–230). T.M.C. Asser Press. DOI: https://doi.org/10.1007/978-94-6265-407-5

**Fakieh, A.,** & **Akremi, A.** (2022). An effective blockchain-based defense model for organizations against vishing attacks. *Applied Sciences*, *12*(24), 13020. DOI: https://doi.org/10.3390/app122413020

**Falade, P.** (2023). Decoding the threat landscape: ChatGPT, FraudGPT, and WormGPT in social engineering attacks. *IJSRCSEIT*, *9*(5), 185–198. DOI: https://doi.org/10.32628/CSEIT2390533

**Girinoto, D. F. P., Yulita, T., Muhammad, A., Rifqi, A. F.,** & **Putri, A. S.** (2022, October). OmeTV pretexting phishing attacks: A case study of social engineering. *In 2022 7th International Workshop on Big Data and Information Security (IWBIS)*, 119–124. IEEE. DOI: https://doi.org/10.1109/IWBIS56557.2022.9924801

**Haggard, S.,** & **Lindsay, J. R.** (2015). North Korea and the Sony hack: Exporting instability through cyberspace. *JSTOR*, *117*.

**Hathaway, M.,** & **Klimburg, A.** (2012). *Preliminary considerations: on national cyber security*. *National Cyber Security Framework Manual*. NATO Cooperative Cyber Defence Centre of Excellence, Tallinn.

**Hoofnagle, C. J., Sloot, B. V. D.,** & **Borgesius, F. Z.** (2019). The European Union general data protection regulation: what it is and what it means. *Information & Communications Technology Law*, *28*(1), 65–98. DOI: https://doi.org/10.1080/13600834.2019.1573501

**Irani, D., Balduzzi, M., Balzarotti, D., Kirda, E.,** & **Pu, C.** (2011). Reverse social engineering attacks in online social networks. *Detection of Intrusions and Malware, and Vulnerability Assessment*. *Lecture Notes in computer Science*, *6739*, 55–74. DOI: https://doi.org/10.1007/978-3-642-22424-9_4

**Ismail, K. A., Singh, M. M., Mustaffa, N., Keikhosrokiani, P.,** & **Zulkefli, Z.** (2017). Security strategies for hindering watering hole cyber crime attack. *Procedia Computer Science*, *124*, 656–663. DOI: https://doi.org/10.1016/j.procs.2017.12.202

**Jain, A. K.,** & **Gupta, B. B.** (2021). A survey of phishing attack techniques, defense mechanisms and open research challenges. *Enterprise Information Systems*, *16*(4), 1–39. DOI: https://doi.org/10.1080/17517575.2021.1896786

**Jakala, M.,** & **Pekkola, S.** (2007). From technology engineering to social engineering. ACM SIGMIS Database: *The DATABASE for Advances in Information Systems*, *38*(4), 11–16. DOI: https://doi.org/10.1145/1314234.1314238

**John, S., Ravichandran, N.,** & **Khan, M. F.** (2018). Electronic medical record for deliverance of effective healthcare delivery: Ethical issues and challenges of digitalization in clinical information and electronic medical records (EMR) management. *IOSR Journal of Business and Management, 20*(3), 106–112. DOI: https://doi.org/10.9790/487X-2003020106

**Kamruzzaman, A., Thakur, K., Ismat, S., Ali, M. L., Huang, K.,** & **Thakur, H. N.** (2023, March 1). Social engineering incidents and preventions. *2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC)*, 0494–0498. DOI: https://doi.org/10.1109/CCWC57344.2023.10099202

**Kathiravan, M., Rajasekar, V., Parvez, S. J., Durga, V. S., Meenakshi, M.,** & **Gowsalya, S.** (2023, February). Detecting Phishing websites using Machine Learning Algorithm. *In 2023 7th International Conference on Computing Methodologies and Communication.* DOI: https://doi.org/10.1109/ICCMC56507.2023.10083999

**Kekulluoglu, D., Magdy, W.,** & **Vaniea, K.** (2020, July). Analysing privacy leakage of life events on twitter. *Proceedings of the 12th ACM Conference on Web Science*, 287–294. DOI: https://doi.org/10.1145/3394231.3397919

**Kiesow Cortez, E.** (2020). Data Breaches and GDPR. *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, 239–256. DOI: https://doi.org/10.1007/978-3-319-78440-3_39

**Krombholz, K., Hobel, H., Huber, M.,** & **Weippl, E.** (2015). Advanced social engineering attacks. *Journal of Information Security and Applications*, *22*(1), 113–122. DOI: https://doi.org/10.1016/j.jisa.2014.09.005

**Kwak, Y., Lee, S., Damiano, A.,** & **Vishwanath, A.** (2020). Why do users not report spear phishing emails? *Telematics and Informatics*, *48*, 101343. DOI: https://doi.org/10.1016/j.tele.2020.101343

**Li, G., Zhou, X.,** & **Cao, L.** (2021). AI Meets Database: AI4DB and DB4 AI. *Proceedings of the 2021 International Conference on Management of Data*. DOI: https://doi.org/10.1145/3448016.3457542

**Mehta, A., Vora, D.,** & **Sachala, H.** (2021). A review of social engineering attacks and their mitigation solutions. *International Journal of Engineering Research & Technology, 10*(10).

**Mitnick, K. D.,** & **Simon, W. L.** (2003). *The art of deception: controlling the human element of security*. New York; Chichester: Wiley.

**Montanez, R., Atyabi, A.,** & **Xu, S.** (2022). Social engineering attacks and defenses in the physical world vs. cyberspace: a contrast study. *Cybersecurity and Cognitive Science*, 3–41. DOI: https://doi.org/10.1016/B978-0-323-90570-1.00012-7

**Morse, E. A., Raval, V.,** & **Wingender, J. R.** (2011). Market price effects of data security breaches. *Information Security Journal: A Global Perspective*, *20*(6), 263–273. DOI: https://doi.org/10.1080/19393555.2011.611860

**Neto, N. N., Madnick, S., Paula, A. M. G. D.,** & **Borges, N. M.** (2021). Developing a global data breach database and the challenges encountered. *Journal of Data and Information Quality*, *13*(1), 1–33. DOI: https://doi.org/10.1145/3439873

**Novak, A. N.,** & **Vilceanu, M. O.** (2019). "The internet is not pleased": Twitter and the 2017 Equifax data breach. *The Communication Review*, *22*(3), 196–221. DOI: https://doi.org/10.1080/10714421.2019.1651595

**Orlando, A.** (2021). Cyber risk quantification: Investigating the role of cyber value at risk. *Risks*, *9*(10), 184. DOI: https://doi.org/10.3390/risks9100184

**Paganini, P.** (2020, March 31). *Holy Water targets religious figures and charities in Asia*. Security Affairs. https://securityaffairs.com/100818/hacking/holy-water-watering-hole-attacks.html

**Patrick, H., van Niekerk, B.,** & **Fields, Z.** (2019). Developing cybersecurity resilience in the provincial government. *Cyber Law, Privacy, and Security: Concepts, Methodologies, Tools, and Applications*, 870–897. DOI: https://doi.org/10.4018/978-1-5225-8897-9.ch041

**Perera, S., Jin, X., Maurushat, A.,** & **Opoku, D.-G. J.** (2022). Factors affecting reputational damage to organisations due to cyberattacks. *Informatics*, *9*(1), 28. DOI: https://doi.org/10.3390/informatics9010028

**Pitman, L.,** & **Crosier, W.** (2024). On the scale from ransomware to cyberterrorism: the cases of JBS USA, colonial pipeline and the wiperware attacks against Ukraine. *Journal of Cyber Policy*, 1–21. DOI: https://doi.org/10.1080/23738871.2024.2377670

**Presthus, W.,** & **Sønslien, K. F.** (2021). An analysis of violations and sanctions following the GDPR. *International Journal of Information Systems and Project Management*, *9*(1), 38–53. DOI: https://doi.org/10.12821/ijispm090102

**Prevezianou, M. F.** (2021). Beyond ones and zeros: Conceptualizing cyber crises. *Risk, Hazards & Crisis in Public Policy*, *12*(1), 51–72. DOI: https://doi.org/10.1002/rhc3.12204

**Quader, F.,** & **Janeja, V. P.** (2021). Insights into organizational security readiness: Lessons learned from cyber-attack case studies. *Journal of Cyber security and Privacy*, *1*(4), 638–659. DOI: https://doi.org/10.3390/jcp1040032

**Roberts, P.** (2010, August 26). Thumb drive attack in 2008 compromised classified U.S. networks. *Threatpost*. https://threatpost.com/thumb-drive-attack-2008-compromised-classified-us-networks-082610/74385

**Salahdine, F., El Mrabet, Z.,** & **Kaabouch, N.** (2021, December). Phishing attacks detection a machine learning-based approach. *2021 IEEE 12th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference*, 0250–0255. DOI: https://doi.org/10.1109/UEMCON53757.2021.9666627

**Salahdine, F.,** & **Kaabouch, N.** (2019). Social engineering attacks: A survey. *Future Internet*, *11*(4), 89. DOI: https://doi.org/10.3390/fi11040089

**Shu, X., Tian, K., Ciambrone, A.,** & **Yao, D.** (2017). Breaking the target: An analysis of target data breach and lessons learned. *ArXiv.org*. DOI: https://doi.org/10.48550/arXiv.1701.04940

**Siadati, H., Nguyen, T., Gupta, P., Jakobsson, M.,** & **Memon, N.** (2017). Mind your SMSes: Mitigating social engineering in second factor authentication. *Computers & Security*, *65*, 14–28. DOI: https://doi.org/10.1016/j.cose.2016.09.009

**Sicard, S.** (2015). North Korean cyber attack on Sony poses tough security questions. *National Defense*, *99*(736), 24–25.

**Smith, M.,** & **Mulrain, G.** (2017). Equi-failure: The national security implications of the Equifax hack and a critical proposal for reform. *Journal of National Security Law and Policy*, *9*, 549.

**Soni, S.,** & **Mathew, R.** (2020). Database security: Attacks and solutions. *Proceeding of the International Conference on Computer Networks, Big Data and IoT (ICCBI-2019)* (pp. 917–925). Springer International Publishing. DOI: https://doi.org/10.1007/978-3-030-43192-1_100

**Sonowal, G., Sharma, A.,** & **Kharb, L.** (2021). Spear-phishing emails verification method based on verifiable secret sharing scheme. *Journal of Information Assurance & Security*, *16*(3).

**Thomas, J. E.** (2018). Individual cyber security: Empowering employees to resist spear phishing to prevent identity theft and ransomware attacks. *International Journal of Business Management*, *12*(3), 1–23. DOI: https://doi.org/10.5539/ijbm.v13n6p1

**Tulkarm, P.** (2021). A survey of social engineering attacks: Detection and prevention tools. *Journal of Theoretical and Applied Information Technology*, *99*(18).

**Vadrevu, P.,** & **Perdisci, R.** (2019). What you see is not what you get. *Proceedings of the Internet Measurement Conference*, 308–321. DOI: https://doi.org/10.1145/3355369.3355600

**Wang, Z., Sun, L.,** & **Zhu, H.** (2020). Defining social engineering in cybersecurity. *IEEE Access*, *8*, 85094–85115. DOI: https://doi.org/10.1109/ACCESS.2020.2992807

**Weaver, B. W., Braly, A. M.,** & **Lane, D. M.** (2021). Training users to identify phishing emails. *Journal of Educational Computing Research*, *59*(6), 073563312199251. DOI: https://doi.org/10.1177/0735633121992516

**TO CITE THIS ARTICLE:**
Ukwadinachi, N. (2025). From Mitnick to Modern Database Threats: Evolution of Social Engineering Tactics and Their Impact on Data Integrity. *Journal of Technology Studies*, *50*(1), 14–29. DOI: https://doi.org/10.21061/jts.438

**Submitted:** 10 February 2025 **Accepted:** 17 June 2025 **Published:** 04 July 2025