iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL
FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 Issue: VII Month of publication: July 2025

DOI: https://doi.org/10.22214/ijraset.2025.73414

Social Engineering in Cybersecurity: A Survey of Behavioral Threats, Detection Models, and Prevention Strategies

Chaitra Morab[1], Laxmi Naik[2], Prof. Vinod R Kokitkar[3]
Dept. of Master of Computer Applications, KLS Gogte Institute of Technology Belagavi, Karnataka, India

Abstract: Social engineering is still one of the most widespread and threatening cyber threats, and it is caused more by human vulnerability than technological weaknesses. Driven by the growing sophistication of threats and the absence of collective perception in the discipline, this research combines three general viewpoints: an in-depth expert interview-based analysis, a conceptual framework proposal to operationalize social engineering in cybersecurity, and a mathematical detection model based on a finite state machine. The initial paper emphasizes the essential role of user awareness in preventing threats, with a finding that organizations will tend to prioritize technical measures over staff education. Based on qualitative interviews with cybersecurity professionals, the research determines that socially engineered attacks take advantage of human trust, resulting in credential theft, ransomware attacks, and data breaches. The second paper resolves conceptual ambiguities for the term "social engineer- ing" through a consideration of its history, suggesting a clear, operational definition, and providing structured comparative models. The third contribution is the development of the Social Engineering Attack Detection Model (SEADM), with an added deterministic finite state machine that classifies attack vectors by communication modes and user responses. This model helps to organize organizational defenses by detecting and stopping social engineering attempts via formalized transitions. Taken together, the results highlight that a multi-faceted approach—integrating awareness, conceptual clarity, and structured detection mecha- nisms—is needed in order to fight the rising threat of social engineering. This intersection of theoretical, conceptual, and pro- cedural innovations presented herein provides a strong platform for both comprehending and countering human-centric cyber threats.

Index Terms: Social Engineering, Cybersecurity, Information Security Awareness, Psychological Manipulation, Social Engineering Attack Detection.

I. INTRODUCTION

In the age of the digital world, cybersecurity remains under constant threat from sophisticated and changing attack pat- terns, one of the most insidious of which is social engineering.

While conventional cyber-attacks involve systems or software vulnerabilities, social engineering plays on human psychology by leveraging cognitive biases, trust, or ignorance. With orga- nizations becoming more digitally oriented in their work, the human factor has remained the weakest link in the security chain. Social engineers circumvent firewalls and encryption by tricking employees into sharing sensitive information or opening up unauthorized access. In addition to strong technical controls, these psychological attacks emphasize the necessity for security measures that target human behavior in conjunc- tion with technical measures [4], [5].

Social engineering has long been a presence in historical times, but its context in cyberspace has become increasingly significant. A report by Aldawood and Skinner reveals that social engineering attacks currently represent 97% of malware- related cases, while only 3% use software vulnerabilities [4]. The complexity of the attacks is increasing, as evidenced by actual case scenarios like Saudi Aramco being hit by the 2012 Shamoon virus, causing oil operations to be disrupted and erasing 35,000 computers. This attack was not a result of a software flaw but a human one—lack of awareness among employees [5]. Such attacks confirm the observation that organizations need to address social engineering as much of a much of a behavioral issue rather than a technical one [8].

Social engineering is effective because it plays on psy- chological characteristics like helpfulness, compliance with authority, or urgency reaction. Attack vectors such as phishing, pretexting, baiting, and impersonation take advantage of these behavioral trends [13].

Recent studies try to classify and comprehend these vectors, including the Social Engineering Attack Detection Model (SEADM), which establishes states such as ”request clarity,” ”identity verification,” and ”authority validation” to analyze systematically the validity of interactions [7]. The model stresses that decision-making on the basis of requests should be context-specific security checks and well-defined response paths, less likely to be exploited.

For furthering understanding and determining best practices, researchers have embarked on a multidisciplinary research methodology merging technical analysis with human-oriented studies. An example is thematic analysis carried out by Aldawood et al. from interviews with cybersecurity experts, which pointed out that solutions are not sufficient on the technical front. In contrast, awareness training, user education, and behavioral modeling became the most supported coun- termeasures [4], [5], [13]. The research also concluded that incorporating training into organizational culture, as opposed to doing it once, results in more enduring resilience against changing social engineering attacks [12].

Survey results indicate that companies are now applying contemporary and dynamic training approaches. Among these are gamification-based learning modules, simulated phishing campaigns, and role-based awareness training [14]. One inno- vative solution is the incorporation of finite state machines in models such as SEADM, which trace out potential request scenarios and user decision routes to assist employees in recognizing and rejecting suspicious behavior [7]. The state- machine infrastructure converts detection from a reactive process to an active decision-making process, enabling employ- ees to evaluate credibility using orderly steps, for instance, authenticating the identity of the requestor or assessing the believability of their assertion [7].

Complications still exist. Awareness programs are not ev- erywhere standardized and effectiveness differs according to organizational environment, roles of users, and frequency of training [6], [12]. Experts in several studies insisted on periodic, role-based refreshes of training material to incorporate emerging threat vectors, i.e., AI-based phishing and deepfake impersonations [9], [10].

Further, some interviewees contended that awareness programs should not be compulsory but crafted to entice willing participation through incentives or enticing content. This change from enforcement to encourage- ment is in line with modern behavioral psychology strategies for learning [18].

Literature also highlights vulnerable populations and high- risk contexts where social engineering is most effective. For example, demographic analysis of phishing susceptibility indi- cates that lower cybersecurity literacy users, such as students and non-technical employees, are likely to be targeted [6], [7]. Awareness campaigns should then target at-risk users and adapt communication according to their cognitive and cul- tural contexts [11]. Incorporating awareness into onboarding procedures, frequent performance reviews, and practice drills maintains constant reinforcement of safe habits [13].

In addition, governmental and institutional backing is nec- essary in the battle against social engineering on a large scale. Prevention can be amplified by governments requiring cybersecurity training in schools and colleges, subsidizing public campaigns, and creating strict compliance standards for organizations dealing with sensitive infrastructure or personal information [2], [3]. The success of such initiatives is con- tingent upon the incorporation of private-sector efforts. For example, antivirus software companies can improve usability and understanding of security functionality, while organiza- tions can implement real-time anti-phishing filtering systems embedded in email platforms [12].

Finally, social engineering is a uniquely human threat to cy- bersecurity—one that technology cannot solve on its own. The increasing amount, sophistication, and insidiousness of these attacks highlight the necessity for holistic, behavior-oriented defenses [1], [4], [13]. An effective avoidance strategy should integrate technical infrastructure, psychological understanding, ongoing user education, and institutional application [5], [14]. A wealth of research indicates a strong correlation between enhanced contextual awareness and reduced vulnerability to social engineering [4], [13]. Thus, through investment in user awareness and the implementation of models such as SEADM, organizations can create a ”human firewall”—an active, educated workforce that can withstand even the most advanced manipulations.

II. LITERATURE REVIEW

In the last ten years (2015–2025), the terrain of social engineering (SE) defense research has evolved from disconnected technical countermeasures to holistic, interdisciplinary frame- works. These integrate cybersecurity tools with behavioral science, human-computer interaction (HCI), and institutional practices. This section categorizes the literature under five domains: (1) taxonomy of SE attack vectors, (2) user-centered training and awareness interventions, (3) cognitive-behavioral modeling of security behavior, (4) decision-state detection models, and (5) institutional and regulatory initiatives.

A. Social Engineering Attack Vectors and Exploited Behavior

SE attacks utilize psychological mechanisms such as trust, fear, and authority to circumvent traditional technical safe- guards [1], [8]. Initial classifications included phishing, bait- ing, and pretexting. Svehla et al. [1] illustrated that these at- tacks rely more on human vulnerability than software exploits. Frumento et al. [8] described a shift toward "semantic at- tacks" that mimic workplace communication, lacking malware payloads but employing sophisticated impersonation. Reddy and Reddy [3] highlighted phishing as a key malware delivery vector that capitalizes on urgency and authority cues. Heartfield et al. [10] introduced the concept of zero-day semantic attacks, which manipulate users through confusion or partial truths, making them unknowing participants in breaches.

B. Training Methodologies and Awareness Frameworks

Awareness training remains the most effective non-technical defense against SE attacks [4], [5]. Aldawood and Skinner [4] reported that approximately 90% of SE incidents result from human error. Embedding awareness into organizational culture—rather than one-time training—yields greater long- term resilience. Sheng et al. [6] found that students and non-technical per- sonnel are more susceptible to SE attacks, a finding reinforced by Farooq et al. [7], who noted that awareness levels are closely tied to background and experience. These insights led to gamified training programs and adaptive phishing simula- tions [14]. Caputo et al. [14] showed that interactive simulation-based learning outperforms passive training in knowledge retention. These simulations incorporate feedback loops akin to rein- forcement learning, allowing real-time behavior correction.

C. Psychological and Cognitive Modeling of Security Behavior

Researchers have increasingly explored psychological dimen- sions to understand why users fall for SE attacks even with prior training. Tsohou et al. [11] emphasized the influence of organizational values and personal motivation on secure behavior. Braun and Clarke [16] applied thematic analysis to uncover latent user perceptions of risk and peer influence. Qualitative studies by Berg and Lune [18], and Miles et al. [17] revealed how factors like stress and organizational hierarchy impact decision-making. Aldawood et al. [4] and Ghafir et al. [13] proposed embedding cognitive-behavioral feedback into daily workflows using metrics and reinforcement loops.

D. Detection Models: SEADM and Decision-State Logic

Real-time detection models complement user awareness by offering structured responses to SE threats. Ghafir et al. [13] proposed the Social Engineering Attack Detection Model (SEADM), which segments decision-making into states such as identity verification, plausibility assessment, and authority confirmation.

The model was later augmented with Finite State Machine (FSM) logic to enable structured user decision pathways. Heartfield et al. [10] validated the "human-as-a-sensor" con- cept, showing that trained users guided by FSM cues could detect even sophisticated SE attempts. Blandford [15] advocated semi-structured models like SEADM that balance automation with human judgment—an approach aligned with modern HCI trends promoting user- driven security interventions.

E. Institutional and Regulatory Role in Defense

Robust SE defense requires institutional and policy alignment. Breda et al. [2] and Reddy et al. [3] called for national-level cybersecurity education and curriculum mandates. Government- driven campaigns and compliance protocols serve as systemic deterrents. In the private sector, Alavi et al. [12] noted the integration of AI-based SE detection in enterprise tools. However, without simultaneous investment in user training and cultural shifts, these tools underperform. Thomas et al. [9] found that cre- dential theft is predominantly a result of SE, underscoring the need for hybrid approaches that blend automation with human awareness.

TABLE I

KEY STUDIES ON SOCIAL ENGINEERING DEFENSE

Ref.	Focus Area	Key Contribution
[1]	Attack Classification	Overview of psychological tech- niques in SEAs
[4]	Awareness Importance	Role-specific training improves organizational resilience

[6]	Demographic Susceptibility	Youth and students more vulner- able to phishing
[10]	Detection Paradigm	Human-as-sensor model for se- mantic attacks
[13]	SEADM Model	Finite state logic for stepwise SEA detection
[14]	Simulation-Based Training	Phishing games improve long-term behavioral change
[15]	HCI-Cognitive Integration	Semi-structured decision support for SEA handling
[12]	Organizational Culture	Security integrated into institu- tional workflows
[2]	Public Sector Role	Advocates for education policies at national levels
[9]	Credential Theft Risks	Emphasizes stolen credentials as byproduct of SEAs

F. Summary of Literature Review

The literature reviewed uniformly explains that technical countermeasures are not enough to counter social engineering. Rather, the most resilient systems combine technical defenses with psychological training, policy enforcement, and formally designed decision-support tools such as SEADM. Adaptive learning, gamified simulation, and role-specific training are demonstrated to enhance resilience, but standardization and generalizability gaps persist. Real-time adaptation, cross-role behavior modeling, and policy-technology synergy need to be addressed in future research in order to develop a scalable defense architecture.

III. METHODOLOGY

Social engineering attacks, as opposed to traditional cyber- attacks, target psychological manipulation instead of software weaknesses. Prevention must therefore cater to human as well as logical defense mechanisms. This method combines two complementary tracks: a formal model called the Social Engineering Attack Detection Model (SEADM) and qualitative perspectives from expert interviews. These two combine to form a human-aware, technically sound, and scalable preven- tion approach. Fig. 1 provides an overview of the conceptual approach: a core decision-making process (SEADM logic) driven by four interconnected layers—behavioral training, formal modeling, organizational design, and thematic field insights. Each of the dimensions brings its specific capabilities in foretelling and countering socially engineered attacks in diversified environ- ments.

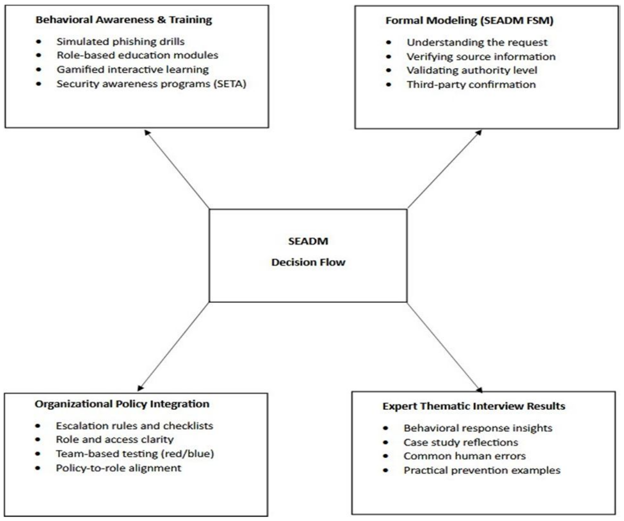
Behavioral Awareness & Training
Simulated phishing drills
Role-based education modules
Gamified interactive learning
Security awareness programs (SETA)
Formal Modeling (SEADM FSM)
Understanding the request
Verifying source information
Validating authority level
Third-party confirmation
SEADM
Decision Flow
Organizational Policy Integration
Escalation rules and checklists
Role and access clarity
Team-based testing (red/blue)
Policy-to-role alignment
Expert Thematic Interview Results
Behavioral response insights
Case study reflections
Common human errors
Practical prevention examples

Fig. 1. Overview of Social Engineering Attack Detection Model (SEADM)

A. SEADM-Based FSM Modeling of Attack Flow

SEADM is a finite state machine (FSM) model employed to mimic how individuals process potentially fraudulent so- cial engineering requests. It is a sequence of states a user must move through before granting or rejecting a request. These states include understanding the request, checking the source, reviewing third-party affirmation, and validating the requester's authority.

Every transition is predicated upon an explicit binary con- dition. If the request is not understandable, the user is advised to reject it. Similarly, if the source cannot be authenticated or the requester's authority level is not verified, the process is terminated. These decision checkpoints reduce the risk of unauthorized access and erroneous approvals. Through this human decision-making modeling, SEADM provides a trust- worthy framework for real-time security awareness training and system integration.

B. Expert Interview-Based Thematic Analysis

Expert interviews with cybersecurity and enterprise IT profes- sionals were conducted to enhance the technical model. The interviews were semi-structured, and data was analyzed using Braun and Clarke's six-step thematic analysis methodology. Insights from the interviews revealed gaps in policy com- munication, employee awareness, training effectiveness, and incident handling.

Recurrent themes included uneven role-specific training, lack of immersive simulations, and ambiguity in escalation processes. These findings show that several employees lack the clarity and confidence needed to handle social engineer- ing incidents. Qualitative inputs help anchor SEADM within practical enterprise environments.

C. Integration of FSM and Thematic Dimensions

Combining SEADM with expert-informed themes ensures that the methodology is both systematic and adaptable. For in- stance, while SEADM mandates third-party verification, expert feedback emphasized empowering employees with the tools and authority to do so. Where FSM suggests rejecting vague requests, thematic insights highlighted that urgency and impersonation tactics often bypass logical reasoning. As a result, FSM logic was extended to include emotional awareness training and context- rich decision support to increase real-world effectiveness.

D. Behavioral Training and Awareness Simulation

Behavior-focused training, modeled on Security Education, Training, and Awareness (SETA) principles, complements SEADM's logic. As supported by [4], [5], and [14], interactive and role-based modules—such as phishing simulations, gam- ified quizzes, role-play exercises, and video storytelling—are more effective than textual guidelines.

These training tools mirror the SEADM decision states, reinforcing user actions like rejecting unverifiable requests or escalating uncertain interactions. This procedural reinforce- ment builds confidence and decision-making fluency among employees.

E. Policy Design and Organizational Structure

Training alone is insufficient without policy backing. This component focuses on creating organizational policies that institutionalize FSM-based decisions. Such policies clearly define roles and decision points—for example, "If authority cannot be verified, escalate," or "Terminate communication if source verification fails."

Policies must reflect employee responsibilities to reduce ambiguity. As shown in [11]–[13], clear policy instructions improve user confidence and response speed. Regular red/blue team exercises can verify compliance and highlight policy loopholes.

F. Communication Channels and Decision Escalation

The presence of secure, responsive communication channels is vital. Expert feedback highlighted that social engineering attempts succeed mostly when employees cannot promptly reach supervisors or IT support.

Hence, secure messaging tools, escalation dashboards, and help hotlines are recommended. These infrastructure tools act as extensions of the FSM logic, providing users immediate support at any decision state.

G. Comparative Evaluation with Other Models

Unlike probabilistic phishing filters or machine-learning-based anomaly detectors, SEADM provides a deterministic, user- centered flow. It guides users through clearly defined decision paths: clarify, verify, and validate.

The model can be embedded in intranet tools, training sim- ulations, or interactive chatbots. However, it needs behavioral reinforcement for effective deployment. Without cultural and organizational support, even a logically sound model may fail in high-stress or novel scenarios.

H. Model Limitations and Generalization

One limitation of SEADM is its insufficient handling of emotional manipulation—such as fear or urgency—which of- ten influences user behavior. While the model accounts for verification failure, it does not adequately simulate scenarios where users feel compelled to comply with authority.

To address this, emotional-context simulations must be introduced during training. Additionally, the assumption of uniform decision capability across roles limits generalizability. FSM parameters should be customized per role, department, and organization type.

I. Summary of Methodology

This approach hybridizes a logic-based FSM model (SEADM) with qualitative expert feedback. FSM ensures rule- based, structured reactions, while behavioral insights introduce practical flexibility. Training content, communication tools, and policy frameworks all follow this unified logic.

IV. CHALLENGES AND OPEN ISSUES

A. Conceptual Ambiguity in Defining Social Engineering

The core challenge brought forward in both sources is the absence of a single and holistic definition of social engineering (SE). Mouton et al. point to the necessity of an ontological framework to standardize language and formalize detection models. In the absence of a shared conceptual base, the cybersecurity community finds it difficult to construct coherent solutions

- Lack of uniformity in usage of the term between aca- demic and industry circles.
- Overuse that results in misapplication of unrelated attacks as social engineering.
- Uncertainty regarding the distinction between social en- gineering and technical exploitation

B. Psychological Weaknesses and Human Vulnerability

The human element is the weakest link in the security chain across the globe. Both Mouton et al. and Aldawood & Skinner recognize cognitive biases and human error as the key vectors targeted by social engineers. Attackers engage emotions of trust, fear, and urgency to circumvent technical controls.

- Predisposition to trust or assist others.
- Disposition to obey perceived authority.
- Overload and lack of attention to detail in procedural tasks.

C. Training Programs: Ineffective and Infrequent

One of the key issues highlighted by industry experts in Skinner's and Aldawood's study is the ineffectiveness of existing awareness training programs. These, though widely popular, do not effectively change user behavior. Experts point out that merely educating users is not enough; users need to be trained to behave differently when stressed or lying

- Lack of personalization and relevance to specific roles.
- Infrequently revised to accommodate current SE methods.
- Performed rarely and with no simulation of real-world.

D. FSM Constraints in Simulating Complex Behavior

Mouton et al. suggest a deterministic finite state machine (FSM) for simulating social engineering detection. Although this is an improvement over earlier non-deterministic models in that it allows for finite results, it is limited by its inflexibility.

Human action cannot be readily modeled as a collection of discrete, predictable states.

- Oversimplification of decision-making processes.
- Failure to represent non-linear or affective influences.
- Scaleability difficulties across various organizational en- vironments to explore.

E. Domain-Specific Adaptability of SEADM

The FSM structure of SEADM includes generalized states such as grasping the request, authenticating authority, and third-party verification. Yet each organization will interpret and apply these states differently depending on its own struc- ture and threat scenario. Mouton et al. recognize this and propose future research into contextual extensions.

- Lack of authoritative direction for tailoring the FSM to particular industries.
- Challenges in accommodating individualized workflows or compliance needs.
- Potential misimplementation or incomplete application.

F. Lack of Standardized Evaluation Metrics

Aldawood and Skinner highlight the necessity for metrics measuring the efficacy of awareness programs and detection systems. Without standard performance measures, organiza- tions are unable to gauge progress or continue to fund SE prevention.

- Lack of behavioral KPIs (e.g., phishing response time).
- No standard for training recall or deception resistance.
- Challenges in correlating training results with actual incident data.

G. Increasing Sophistication of Attack Methods

Social engineering methods have moved much beyond simple phishing. Aldawood and Skinner discuss threats such as spear-phishing, pretexting, deepfakes, and multi-step campaigns modeling normal workflow. Mouton et al. also acknowledge that SEADM needs to be updated on a continuous basis to keep up with what is new.

- Support from AI to create hyper-real messages or voices.
- Exploiting publicly available information from social media.
- Mixing SE with technical exploits for hybrid attacks.

H. Technical Detection is Not Sufficient Alone

Mouton et al. believe that although FSM frameworks such as SEADM are beneficial, they need to be complemented with user training and organizational awareness. Aldawood and Skinner attest to the same, stating that strictly technical controls do not identify manipulation that takes place through legitimate communication channels.

- Lack of detection of psychological manipulation.
- Verbal or face-to-face interactions missed cues.
- Illusion of security because of software tool overdepen- dence.

I. Real-Time Response Mechanisms Are Absent

The majority of SE defense tactics are defensive in nature, not proactive. Both sources note that damage is already inflicted before a social engineering attack is actually noticed. There is an increasing demand for tools that can aid users in decision- making during real-time interactions.

- Lack of real-time support for employees who deal with sensitive requests.
- No dynamic warning systems when communication is in progress.
- Delays in reporting cause incidents to escalate.

J. Gaps in Organizational Culture and Leadership

Experts in Aldawood and Skinner’s research believe that awareness programs and training programs flop because of the absence of leadership sponsorship and poor organizational se- curity culture. Mouton et al. state that in order for SEADM to succeed, it has to be incorporated within a wider institutional framework.

- Lack of buy-in for training budgets and compliance by executives.
- Leadership poor modeling of security behavior.
- Inconsistent policy communication and enforcement.

K. Challenge in Adapting FSM to New Threat Situations

Mouton et al.’s FSM design, although robust for well-known SE patterns, does not have an embedded mechanism to handle new or emerging threats. State transitions need to be manually revised by organizations, which brings risk and inconsistency into the scenario.

- FSM states are not dynamic or self-learning.
- No integration with threat intelligence feeds or machine learning.
- Expert revision necessary for every new attack vector.

L. Awareness Decay Over Time

Aldawood and Skinner indicate that awareness training follows a decay curve. Employees tend to fall into risky behavior a few months following training unless reinforced.

Organizational resilience will reduce without periodic retraining.

- Insufficient follow-up or reinforcement systems.
- No gamification or engagement plans.
- Not testing retention using real-time simulations.

M. Inequitable Training Across Employee Roles

Security awareness is usually rolled out consistently to all de- partments, disregarding role-based exposure to risk. Aldawood and Skinner suggest varying training content depending on employees' job functions and threat levels.

- Executives subject to impersonation attacks.
- IT personnel exposed to SE technical threats.
- Customer service handling pretexting and emergency requests.

N. Challenges Integrating SEADM into Daily Operations

While SEADM is conceptually sound, Mouton et al. ac- knowledge it is difficult to implement within actual business settings. Organizations have to take the FSM and convert it into procedural processes without affecting workflows.

- Translating FSM states to decision trees in actual life.
- Educating personnel to adhere to state-based procedures under stress.
- Integrating FSM into software applications and commu- nication tools.

O. Reactive Posture Instead of Preventive Strategy

Most organizations deal with SE threats only after a breach. Both authors suggest moving towards prevention by means of policy, awareness, and proactive detection. This cultural shift is still an open challenge.

- No prior-screening of communication for social engineer- ing patterns.
- Inadequate proactive red teaming and emulated SE at- tacks.
- Limited use of deception technologies to ensnare social engineers.

P. Call for Multi-Layered, Human-Centric Defense Models

At the end, the two studies concur that combating social engineering demands an integrated model that incorporates be- havioral awareness, technical detection, and firm governance. The future work should incorporate models such as SEADM with user-specific interventions and organizational maturity models.

- The integration of FSM with adaptive training modules.
- Employing machine learning to identify user behavior anomalies.
- Developing policies that connect detection, reporting, and user feedback loops.

V. FUTURE DIRECTIONS

A. Enhancing the SEADM Model for Real-World Applicabil- ity

The SEADM model presented by Mouton et al. is a seminal framework for the detection of social engineer- ing attempts, particularly through its disciplined FSM implementation. Ef- fective in principle, its application in real-world organizations requires scalability, responsive- ness, and domain-specific cus- tomization enhancements. Areas for improvement:

- Automating FSM transitions according to changing threat patterns.
- Facilitating modularity for adapting to varying in- dustry environments.
- Embedding real-time decision prompts into commu- nica- tion tools.

By adapting the SEADM beyond academic scenarios, it can become an effective operational tool for mitigating SE threats in complex, fast-moving settings.

B. Incorporating Behavioral Learning Mechanisms into FSM Models

One of the fundamental limitations in current SEADM is its use of static transitions that don't change with user activity or organizational evolution. Incorporating machine learning or reinforcement learning into FSM logic represents a significant path to adaptive, intelligent SE detection.

Future work may involve:

- User interaction-based feedback loops for SE at- tempts.
- Behavior-based state relevance updates to FSM.
- Synching with organizational threat history and analysis.

With such improvements, the FSM would adapt as it ”learns” from both effective and ineffective defenses, building a more personalized and precise detection sys- tem.

C. Domain-Specific Implementations and Guidelines

Mouton et al. highlight the versatility of SEADM, but its real- world application in industries such as healthcare, finance, or education still lacks specific adaptation pro- cesses. Ev- ery domain contains particular workflows and risk factors, demanding corresponding FSM transitions and verification procedures.

- Healthcare-specific states (e.g., validation of a pa- tient data request).
- Financial-sector transitions with multi-level ap- provals.
- Academic workflows with focus on public data access risk.

Supplying sector-specific implementation guides will help to ensure the model is suitably contextualized and implemented effectively within different organizational structures.

D. Expanding Real-Time Detection Capabilities

One of the notable gaps pointed out by Aldawood and Skinner is the absence of real-time utilities that warn or support users in the midst of ongoing SE attempts. The work ahead must focus on the design of systems capable of identifying and counteracting threats in real time. Examples of proposed innovations are:.

- Smart email and chat plugins that analyze messages for signs of manipulation.
- AI-powered warnings that analyze the authenticity of requests in real-time conversations.
- In-system prompts leading employees through FSM state verifications.

By giving real-time instructions, users are better equipped to make informed decisions, minimizing chances for manipula- tion in high-pressure social engi- neering situations.

E. Context-Aware Awareness Program Development

Training programs tend to be too generic and do not account for specific user roles or organizational settings. Aldawood and Skinner emphasize the importance of context-aware training consistent with the user’s envi- ronment and particular expo- sure to SE threats. Successful improvements could include

- Role-specific content that mirrors real job duties.
- Personalized phishing simulation based on prior user mistakes.
- Adaptive modules activated by monitoring behavior.

Customized training makes it relevant, enhances user in- volvement, and hence increases the retention of essential SE prevention techniques.

F. Gamified and Scenario-Based Learning Platforms

One of the foremost recommendations from the expert inter- views is the use of gamified and scenario-based training to enhance user engagement. Lectures and text- books are not effective in readying users against actual social engineering attempts.

- Virtual environments that mimic multi-step SE at- tacks.
- Point systems and leaderboards for competition in train- ing engagement.
- Dynamic role-playing exercises that mimic imper- sonation or pretexting.

Simulation-based training is conducted to give employ- ees hands-on experience, allowing them to react more efficiently when faced with real threats.

G. Recursive and Periodic Awareness Reinforcement

Cybersecurity awareness will also decrease over time if the training is only done once or twice a year. Alda- wood and Skinner propose that organizations require an ongoing education program that reminds employees of key principles periodically.

Continuous learning strategies:

- Weekly ”micro-lessons” through mobile or email.
- Monthly in-house phishing exercises with auto- mated feedback.
- Quarterly threat briefings tailored to each depart- ment.

Continuous reinforcement counters knowledge obsoles- cence and promotes a security-aware culture that is immunized against changing SE tactics.

H. Unified Metrics for Measuring SE Preparedness

Both articles recognize the absence of normalized met- rics to assess user preparedness against SE threats. Creating these metrics is a high priority for future benchmarking of aware- ness effectiveness and informing training optimization. Some potential metrics are:

- Phishing simulation click rates and reporting times.
- Decision accuracy under simulated stress.
- Behavioral risk scores tied to performance in the real world.

Standardized assessment tools will enable cleaner com- parisons between teams and industries and identify areas of strength and weakness in SE defense

I. Policy-Supported Organizational Models

Social engineering defense is frequently undermined by weak policy enforcement or lack of management buy-in. Aldawood and Skinner advocate for a policy framework that supports SE resilience through institutional design. Policy components required:

- Compulsory SE training as part of onboarding and annual appraisals.
- Executive sponsorship and role modeling of safe behav- ior.
- Policy enforcement mechanisms for policy breaches.

Policies that facilitate training, enhance reporting, and hold users accountable foster an environment in which SE threats are addressed with the gravity they merit.

J. Embedding SEADM into Business Workflows

Embedding SEADM into Business Workflows In order to enact SEADM, future efforts need to embed it into workflows within employees directly. Instead of existing as a standalone tool, the FSM model should inform day-to-day processes and decision points. Embedding opportunities include:

- Incorporating FSM logic into customer service tick- eting systems.
- Synchronizing email validation processes with FSM state checks.
- Incorporating FSM stages into standard operating proce- dures.

Smooth integration means that social engineering detec- tion becomes the default part of employee behavior, not extra overhead.

K. Dynamic Models That Reflect Emerging SE Patterns

Social engineering techniques are always changing, but FSM- based models such as SEADM must be updated manually to keep up. Automating the process of updat- ing with threat intelligence will make the model more sustainable and appli- cable. Areas for improvement:

- Tying FSM input to real-time phishing feeds and alerts.
- Auto-creating new state transitions from attacker behavior data.
- Tapping into machine learning to recognize patterns in fresh SE techniques.

These agile systems will enable organizations to remain in front of attackers through the evolution of detection models to keep pace with current threat trends.

L. Technical-Behavioral Collaboration

Aldawood and Skinner highlight that SE defense calls for collaboration among technical, training, and HR departments. Emerging frameworks need to focus on interdisciplinary col- laboration and not fragmented ap- proaches. Suggested col- laboration models:

- Cross-departmental cybersecurity committees.
- Collaborative development of training and detection

- Common reporting platforms that record both hu- man and technical activities.

By coordinating the efforts of technologists, educators, and policy-makers, organizations can launch a more con- certed and effective defense against social engineering.

M. Globalization of SE Detection Standards

International companies and global communications mean that SE attacks know no borders. Inconsistency in standards among regions can lead to inconsistency in detection and training. Future objectives should be:

- Establishing ISO-style standards for the prevention of SE and training.
- Translation-ready awareness materials.
- Translation-ready awareness materials.

Harmonized global action will enable more robust cross- border partnerships and minimize differences in SE defense maturity.

N. Creating Realistic, Ethical SE Simulations

While simulated phishing and pretexting exercises are vital for training purposes, they can have a negative backlash if not developed ethically. Future efforts need to strike a balance between realism and consideration for employee welfare. Ethical concerns are:

- Transparent opt-in consent.
- Steering clear of high-stress or career-risking situa- tions.
- Making simulations educational, rather than puni- tive.

Responsible simulation design will foster greater partic- ipa- tion and avert backlash potentially eroding trust in security teams.

O. Building a Culture of Shared Responsibility

Culture has an important role to play in SE defense. Both papers contend that users need to be made to feel responsi- ble—rather than just required—to defend information assets. Future work has to be aimed at instilling SE awareness within organizational values. Steps to develop a shared culture:

- Reward systems for reporting suspicious activity.
- Public awarding of employees who help avoid SE inci- dents.
- Peer-initiated awareness programs and mentoring.

Establishing a culture in which security is shared respon- sibility minimizes reliance on any one point of defense and fosters an atmosphere of watchfulness.

VI.DISCUSSION

The popularity of social engineering as a threat to cyberse- curity continues to grow, primarily because it exploits human vulnerabilities rather than technological flaws. Through expert interviews conducted in this qualitative study, it was revealed that modern social engineering attacks employ manipulation strategies such as phishing, impersonation, ransomware, and data breaches. Experts consistently noted a key distinction: while technical attacks can be mitigated through security tools, social engineering targets user behavior, often bypassing even the most robust cybersecurity infrastructures. The inability of users to detect subtle threats or understand the risks of seemingly benign interactions was frequently cited as the root cause of security breaches.

Experts highlighted phishing emails as one of the most prevalent and harmful social engineering techniques. Partici- pants described such attacks as increasingly sophisticated and psychologically manipulative—leveraging urgency, authority, and fear to coerce targets into compromising actions. A critical observation was that organizations invest heavily in technological solutions while neglecting the human aspect of security. One expert remarked that user awareness must be prioritized equally with system updates, stating, “there is no button to enable the human firewall.”

Additionally, most participants agreed that social engineer- ing thrives on user ignorance. Victims often lack awareness of how breaches occur or the implications of credential ex- posure. Social engineers exploit trust and unfamiliarity more than systemic flaws. High-profile cases involving platforms such as Facebook, Uber, Adobe, and LinkedIn were cited to illustrate the significant consequences of individual user errors. Interviewees also emphasized the growing complexity of threats, including the use of counterfeit antivirus software and AI-powered impersonations to deceive users.

The Social Engineering Attack Detection Model (SEADM), introduced in the second paper, was identified as a structured response to these challenges. SEADM employs a deterministic finite state machine (FSM) that systematically evaluates each phase of an interaction to determine legitimacy. It categorizes attacks by communication type—unidirectional, bidirectional, and indirect—and defines logical transitions across stages such as request recognition, identity verification, authority valida- tion, and contextual confirmation. This FSM approach enables organizations to intercept manipulation attempts through a reproducible decision-making process.

Findings from both the qualitative interviews and SEADM reinforce that technology alone cannot combat social engi- neering. Experts unanimously advocated for comprehensive user education and behavioral training. Commonly suggested measures included routine phishing simulations, development of custom anti-phishing filters, and incorporation of aware- ness modules into onboarding programs. Experts also rec- ommended cultivating a security-aware organizational culture. Some proposed gamification strategies to enhance engagement and retention in threat recognition exercises.

The analysis further identified limitations in one-time train- ing approaches. Interviewees stressed that awareness programs must be continuous to remain effective. Without regular re- inforcement, users revert to insecure behaviors. One expert commented, “User awareness programs have proved effective in my organization. We observed significant improvement in identifying and reporting phishing attempts following contin- uous training.” Another expert recommended monthly training for general staff and annual refreshers for technical personnel, aligned with varying levels of risk exposure.

Government and educational institutions were also seen as pivotal in establishing long-term cybersecurity resilience. Respondents suggested that digital literacy and social engi- neering awareness should be integrated into school curricula and carried forward into professional environments. National awareness campaigns, standardized training protocols, and public-private collaboration were proposed as government-led measures to strengthen public cybersecurity posture.

The SEADM framework was presented as a technical em- bodiment of these awareness initiatives. Its FSM structure comprises states such as request understanding, requester ver- ification, authority validation, and third-party authentication. Each state functions under Boolean conditions to determine whether a request can proceed. For instance, if a request is not fully understood ($\neg \boldsymbol{U}$), it transitions to a clarification state ($\boldsymbol{S}_2$); if the requester fails identity verification, the process terminates in a failure state ($\boldsymbol{S}_F$). This logical structuring en- sures that decisions are based on policy rather than subjective judgment.

While SEADM provides a robust technical model, experts emphasized its effectiveness is maximized when paired with human-centered training. Participants cautioned against user complacency following isolated training events, advocating for role-specific training and periodic simulated attacks to maintain readiness. Organizations must test both FSM logic and user alertness to maintain a dynamic defense posture.

Summary of Discussion

The consensus across both studies affirms that the human el- ement remains the most exploitable point in cybersecurity. So- cial engineering—despite its non-technical nature—continues to be among the most effective attack methods due to its reliance on manipulating human behavior. While technical models like SEADM offer necessary structure and logic, their success is inherently tied to user awareness and behavioral adaptation. Sustainable prevention strategies must combine deterministic frameworks such as FSMs with continuous train- ing, institutional policy enforcement, and a culture of security. The integration of human and machine intelligence represents the most resilient approach to addressing the evolving threat landscape of social engineering. Together, they offer a technically rigorous and human- relevant defense mechanism against social engineering. This two-pronged approach bridges the gap between theoretical security design and human vulnerability, creating a proactive, adaptive protection model.

VII. CONCLUSION

Social engineering has proven to be one of the most en- during risks in contemporary cybersecurity because it attacks human psychology directly over technological vulnerabilities. In contrast to traditional cyberattacks that take advantage of software vulnerabilities, social engineering attacks play with human trust and behavior, making even most secure systems risky when human users are ill-trained or ignorant. As digital worlds become more complex and interconnected, tackling this human element is becoming a more and more vital component of cybersecurity policy. Studies have proven that conventional technical defenses, while being necessary, are not enough by themselves to counter manipulation-based attacks. Antivirus software, fire- walls, and intrusion detection systems are incapable of keeping track of the sophisticated psychological strategies employed by social engineers. Therefore, user awareness, regular train- ing programs, and behavior-based measures are universally recognized as the best countermeasures. Security Education, Training, and Awareness (SETA) programs and simulated phishing campaigns have been particularly useful in increasing awareness and lowering susceptibility by employees.

Innovative frameworks such as the Social Engineering At- tack Detection Model (SEADM) strengthen defense even fur- ther by providing structured, decision-oriented methodologies that formalize the way people should evaluate and react to dubious requests. Similarly, conceptual elucidations such as the accurate definition of social engineering in cybersecurity (SEiCS) make the phenomenon more practically understood. The combination of these instruments assists organizations in shifting from reactive to proactive defense strategies, al- lowing timely detection and disruption of social engineering campaigns.

Even with these developments, various limitations continue to exist. A significant percentage of the literature that exists today is based upon qualitative data, expert judgments, and anecdotal evidence. Although valuable in nature, such infor- mation is deprived of statistical strength and generalizability to enable the formulation of universally applicable counter- measures. In addition, most established frameworks have not yet been tested across various industries or cultural settings, leaving doubts regarding their applicability and efficacy in different organizational settings. The ever-changing threat landscape only makes prevention more challenging. New technologies like AI-driven chatbots, deepfakes, and large-scale IoT networks are presenting new fronts for social engineering. Attackers today use highly targeted and context-specific tactics, where it becomes increas- ingly difficult to distinguish between normal and attack traffic. In this changing landscape, detection models and awareness programs also need to be updated and improved to remain relevant and useful. Subsequent research will be required to empirically validate existing models and investigate integrating more advanced technologies into user awareness programs. This encompasses the use of machine learning to detect behavior anomalies, blockchain for data integrity verification, and creating adaptive, game-based training platforms to mimic actual-world attack vectors. Furthermore, measuring awareness and behavioral change will be critical in creating standardized metrics for determining the effectiveness of training interventions in the long term. In summary, social engineering is an inherently people- focused threat in cybersecurity. To deal with it effectively is to require a comprehensive approach that bridges technology protection with substantive investment in human education and behavioral modeling. Future defense against social engineering is not in opting between man and machine, but in unifying the two for the creation of strong, security-aware organizations.

REFERENCES

[1] Z. L. Svehla, I. Sedinic, and L. Pauk, “Going white hat: Security check by hacking employees using social engineering tech- niques,” in Proc. 39th Int. Conv. Inf. Commun. Technol., Elec- tron. Microelectron. (MIPRO), May 2016, pp. 1419–1422, doi: 10.1109/MIPRO.2016.7522362.

[2] F. Breda, H. Barbosa, and T. Morais, “Social engineering and cyber security,” in Proc. EM Conf., Int. Technol., Educ. Develop. Conf., 2017,

[3] pp. 1–8.

[4] G. N. Reddy and G. J. U. Reddy, “A study of cyber security chal- lenges and its emerging trends on latest technologies,” arXiv preprint arXiv:1402.1842, 2014.

[5] H. Aldawood and G. Skinner, “Educating and raising awareness on cyber security social engineering: A literature review,” in Proc. IEEE Int. Conf. Teach., Assessment, Learn. Eng. (TALE), Dec. 2018, pp. 62–68, doi: 10.1109/TALE.2018.8615162.

[6] H. Aldawood, T. Alashoor, and G. Skinner, “Does awareness of social engineering make employees more secure?” Int. J. Comput. Appl., vol. 177, no. 38, pp. 45–49, Feb. 2020, doi: 10.5120/ijca2020919891.

[7] S. Sheng, M. Holbrook, P. Kumaraguru, L. F. Cranor, and J. Downs, “Who falls for phish?: A demographic analysis of phishing susceptibility and effectiveness of interventions,” in Proc. 28th Int. Conf. Hum. Factors Comput. Syst. (CHI), 2010, pp. 373–382.

[8] A. Farooq, J. Isoaho, S. Virtanen, and J. Isoaho, “Information security awareness in educational institution: An analysis of students’ individual factors,” in Proc. IEEE Trustcom/BigDataSE/ISPA, vol. 1, Aug. 2015,

[9] pp. 352–359, doi: 10.1109/Trustcom.2015.394.

[10] E. Frumento et al., “The Role of Social Engineering in the Evolution of Attacks.

[11] K. Thomas et al., “Data breaches, phishing, or malware?: Understanding the risks of stolen credentials,” in Proc. ACM SIGSAC Conf. Comput. Commun. Secur. (CCS), 2017, pp. 1421–1434.

[12] R. Heartfield, G. Loukas, and D. Gan, “An eye for deception: A case study in utilizing the human-as-a-security-sensor paradigm to detect zero-day semantic social engineering attacks,” in Proc. IEEE 15th Int. Conf. Softw. Eng. Res., Manage. Appl. (SERA), Jun. 2017, pp. 371–378.

[13] A. Tsohou, M. Karyda, and S. Kokolakis, “Analyzing the role of cognitive and cultural biases in the internalization of information se- curity policies: Recommendations for information security awareness programs,” Comput. Secur., vol. 52, pp. 128–141, Jul. 2015.

[14] R. Alavi, S. Islam, H. Mouratidis, and S. Lee, “Managing social engi- neering attacks—considering human factors and security investment,” in Proc. HAISA, 2015, pp. 161–171.

[15] I. Ghafir et al., “Social engineering attack strategies and defence approaches,” in Proc. IEEE 4th Int. Conf. Future Internet Things Cloud (FiCloud), Aug. 2016, pp. 145–149, doi: 10.1109/FiCloud.2016.28.

[16] D. D. Caputo et al., “Going spear phishing: Exploring embedded training and awareness,” IEEE Secur. Privacy, vol. 12, no. 1, pp. 28–38, Jan. 2014.

[17] A. Blandford, “Semi-structured qualitative studies,” in The Encyclopedia of Human-Computer Interaction, 2nd ed., M. Soegaard and R. F. Dam, Eds. Aarhus, Denmark: The Interaction Design Foundation, 2013.

[18] V. Braun and V. Clarke, “Using thematic analysis in psychology,”

[19] Qualitative Res. Psychol., vol. 3, no. 2, pp. 77–101, Jan. 2006.

[20] M. B. Miles et al., Qualitative Data Analysis: A Methods Sourcebook, 3rd ed. Thousand Oaks, CA: SAGE, 2014.

[21] B. L. Berg and H. Lune, Qualitative Research Methods for the Social Sciences, 8th ed. Harlow, U.K.: Pearson, 2012, p. 408.