Monica Sahni, PhD[*]
Reva Kalra[**]

DOI: 10.51204/Zbornik_UMKP_25134A
Originalni naučni rad

THE SCIENCE OF SOCIAL ENGINEERING: A LEGAL AND BEHAVIORAL PERSPECTIVE ON CYBERSECURITY AWERENESS

Abstract: Social engineering attacks, responsible for over 80% of successful cyber intrusions, exploit human psychology to bypass technical defenses. This research investigates the underlying behavioral mechanisms of social engineering and their implications for cybersecurity law and policy. Combining psychological experiments with statistical analyses of phishing and business email compromise (BEC) incidents, the study identifies key cognitive biases, such as trust manipulation and decision fatigue, that attackers leverage. Additionally, the research examines the role of legal frameworks in mitigating these attacks, focusing on liability allocation, regulatory enforcement, and victim protection. By integrating findings from behavioral science and legal studies, the paper proposes a comprehensive model for cybersecurity awareness, emphasizing targeted training, adaptive policy design, and public-private collaboration. This evidence-based approach aims to reduce the global impact of social engineering attacks while informing future legal and educational strategies.

Keywords: social engineering, cybersecurity, phishing, business email compromise (BEC) incidents victim protection.

1. INTRODUCTION

In today's ever evolving digital cyberspace, cybersecurity threats continue to increase in terms of complexibility and scalability. Among these, one of the most ongoing and deceptive forms of attack is rooted not in the technical vulnerabilities

[*] Researcher, Jindal Global Law School, O P Jindal Global University, Sonepat, India, monicasahni@gmail.com.

[**] Research Officer, Sumona Institute of Behavioural Sciences and Performance Excellences, New Delhi, India.

but in human psychology: social engineering. The manipulation of human behavior to illegally access data, systems, or physical spaces, has become a primary source employed in cybercrime.[11] Recent statistics reveal its prevalence, with over 80% of successful cyber intrusions now involving some type of social engineering – ranging from phishing and business email compromise (BEC) to pretexting and baiting attacks.[2] The successfulness of these strategies lies not in the breakdown of digital infrastructure but in the exploitation of human cognitive biases, decision-making heuristics, and emotional triggers.

Social engineering bypasses the mechanisms which were used by conventional cyberattacks entirely by targeting individuals. Cybercriminals have trained themselves to manipulate trust, urgency, perceived authority, or fear, prompting individuals to share personal information or carry out unauthorized actions. Psychological researches throughout the years have highlighted how factors like trust manipulation, decision fatigue, and attentional overload serve as crucial tools for social engineers.[3] Tactics like these are especially effective in high-pressure environments, such as corporate offices, where individuals are overwhelmed with information and face mounting demands for quick response. There is a pressing need to merge behavioral science to legal regulatory frameworks to create a more robust cybersecurity space.

Despite the growing awareness, existing legal measures often lag in providing comprehensive solutions to social engineering threats. This review seeks to address this interdisciplinary divide by understanding the behavioral roots of social engineering and investigating how legal measures can improve to better mitigate these risks. This study presents a multidisciplinary model aimed at enhancing our comprehension and response to these threats. Specifically, it will

- Recognize and analyze the cognitive biases most commonly exploited in social engineering.
- Assess the efficacy and drawbacks of current legal approaches to cybersecurity.
- Propose an integrated model for awareness training, policy development, and cross-sectoral collaboration.

2. METHODOLOGY

2.1. Research Design

Our paper follows a systematic review design focused on interdisciplinary literature concerning the behavioral and legal dimensions of social engineering

[1] C. Hadnagy, *Social engineering: The science of human hacking*, 2nd ed., Indianapolis, Wiley, 2018.

[2] Verizon, *Data Breach Investigations Report 2023*, *https://www.verizon.com/business/resources/reports/dbir/*

[3] Parsons *et al.*, "Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)", *Computers & Security*, 42/2015, 165–176.

in cybersecurity. The review is grounded in the PRISMA guideline[4] to ensure transparency, reproducibility, and methodological rigor.

2.2. Data Sources and Search Strategy

A comprehensive literature search was conducted using academic databases including:

- **Scopus**
- **Web of Science**
- **PubMed**
- **IEEE Xplore**
- **PsycINFO**
- **LexisNexis** (for legal case law and policy papers)
- **Google Scholar** (for grey literature and government reports)

Search terms included combinations of keywords such as:

- "social engineering"
- "cybersecurity awareness"
- "phishing"
- "business email compromise"
- "cognitive bias"
- "cyber law"
- "legal framework AND cybersecurity"
- "trust manipulation"
- "decision fatigue AND cybercrime"

Boolean operators (AND, OR) were applied to refine search queries, while publication date filters (2005–2024) were used to capture both foundational literature and recent developments relevant to the study.

2.3. Inclusion and Exclusion Criteria

Inclusion Criteria:

- Peer-reviewed journal articles, government reports, and legal case studies.
- Publications in English.
- Studies addressing psychological or legal aspects of social engineering.
- Empirical studies, literature reviews, or theoretical papers.

Exclusion Criteria:

- Non-English publications.
- Papers focused solely on technical solutions (e.g., firewalls or encryption) without behavioral or legal analysis.
- Duplicate records.

[4] Page M. J. *et al.*, "The PRISMA 2020 statement: An updated guideline for reporting systematic reviews", *BMJ,* 372, 71/2021.

2.4. Data Extraction and Synthesis

A standardized data extraction sheet was used to collect the following information from each article:

- Author(s) and year of publication
- Research design and methodology
- Key behavioral constructs (e.g., trust bias, cognitive overload)
- Legal frameworks or case law discussed
- Cybersecurity domain (e.g., phishing, BEC, ransomware)
- Implications for policy or public awareness

Data were synthesized narratively, organizing the findings thematically across behavioral insights, legal interpretations, and policy recommendations. Quantitative patterns such as frequency of discussed biases or prevalence of legal doctrines were also noted where applicable.

3. LITERATURE REVIEW

3.1. The Behavioral Foundations of Social Engineering

Social engineering arises from psychological manipulation, where the cybercriminals tend to work on predictable patterns in human cognition, emotion, and behavior. A growing body of research claims how attackers systematically leverage cognitive biases of humans – such as authority bias, the urgency effect, and trust heuristics – to promote the success rate of phishing and Business Email Compromise (BEC) schemes.[5]

Decision fatigue is a psychological state where focused and sustained decision-making depletes cognitive resources of an individual declining their potential to critically assess information. Usually, corporate employees who face cognitive overload are more likely to click malicious links or disclose sensitive information.[6]

Low self efficancy when it comes to cybersecurity also plays a pivotal role since it correlates with diminished threat recognition and slower response times, increasing susceptibility to manipulation.[7] These findings underpin the importance

[5] P. Kumaraguru *et al.*, “Teaching Johnny not to fall for phish”, *ACM Transactions on Internet Technology (TOIT),* 2/2009, 7; K. Parsons *et al.*, “Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)”, *Computers & Security*, 42/2013, 165–176.

[6] R. F. Baumeister, K. D. Vohs, D. M. Tice, “The strength model of self-control”, *Current Directions in Psychological Science,* 6/2008, 351–355; R. Heartfield, G. Loukas, “A taxonomy of cyber-physical threats and impact in the smart home”, *Computers & Security,* 78/2016, 398–428.

[7] N. A. G. Arachchilage, S. Love, “Security awareness of computer users: A phishing threat avoidance perspective”, *Computers in Human Behavior,* 38/2014, 304–312.

of integrating psychological insight into cybersecurity practices, suggesting that effective defense strategies must go beyond technical framework to include behavioral awareness and training.

3.2. Legal Dimensions of Social Engineering: Gaps and Controversies

The legal dimension to social engineering remains largely **fragmented.** While the national laws in various nations focus on data protection, they often are devoid of targeted provisions addressing **behaviorally-driven cybercrime**. For example, the European Union's **General Data Protection Regulation (GDPR)** mandates strict data governance but does not specifically cover manipulation-based attacks unless they result in personal data breaches.[8]

Legal scholars have voiced for a **shared responsibility model**, particularly when organizations fail to provide adequate employee training or implement preventive safeguards.[9]

Furthermore, while traditional frameworks are effective in adjudicating fraud, newer forms of social engineering challenge established definitions of "reasonable foresight" and "informed consent" in digital contexts.[10]

3.3. Intersections of Behavioral Science and Cyber Law

The integration of behavioral science into cybersecurity law and policy has come into being. Psychological theories such as the **Theory of Planned Behavior**[11] and **Protection Motivation Theory**[12] help support the claim of why individuals stay under threat to scams even when they possess general knowledge about cybersecurity.

Behavioral insights are slowly being integrated into regulatory practices. The United Kingdom's **National Cyber Security Centre (NCSC)**, for example, advocates for "**security by design**" principles that align digital interfaces with

[8] European Parliament, *Regulation (EU) 2016/679 of the European Parliament and of the Council.* General Data Protection Regulation (GDPR), 2016, https://eur-lex.europa.eu/eli/reg/2016/679/oj

[9] D. J. Solove, D.K. Citron, „Risk and anxiety: A theory of data-breach harms", *Texas Law Review,* 4/2017, 737–786.

[10] S. W. Brenner, *Cybercrime: Criminal threats from cyberspace*, Praeger, Santa Barbara – Denver – Oxford, 2010.

[11] I. Ajzen, "The theory of planned behavior", *Organizational Behavior and Human Decision Processes,* 2/1991, 179–211.

[12] P. W. Rogers, "Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation", *Social Psychophysiology* (eds. J. Cacioppo, R. Petty), Guilford Press, New York, 1983, 153–176.

cognitive ergonomics.[13] Courts often work on assessing cognitive manipulation if they happen.

Moreover, both **legal awareness** and **public education campaigns** frequently miss the psychological underpinnings of manipulation. This oversight leads to generating a "**blame-the-victim**" narrative that is not only ineffective in prevention efforts but also ethically troubling.[14]

3.4. Policy Approaches and Institutional Challenges

As far as the policies are considered, there has been a multi-faceted strategy to combat social engineering risks. Effective responses include:

- **Compulsory cybersecurity training** designed to address common cognitive biases which arise.
- **Adaptive legal rules and regulations** that formally identify psychological manipulation as a distinct category of cyber threat
- **Cross-sector partnership** where public institutions, private enterprises, and behavioral science researchers are the stakeholders[15]

4. RESULTS

Summary Table of Reviewed Studies

Author(s) & Year	**Focus Area**	**Study Design**	**Key Behavioral Constructs**	**Legal/Policy Focus**	**Cyber Threat Domain**	**Key Findings**
Kumaraguru *et al.* (2009)	Phishing susceptibility	Experimental	Trust heuristics, urgency	Usertraining implications	Phishing	Simulated training improved phishing detection
Baumeister *et al.* (2008)	Decision fatigue	Theoretical/ Psychological	Cognitive overload	Indirectlegal implications foremployee training	General SE tactics	Fatigue impairs rational decision-making
Heartfield & Loukas (2016)	Cyber-physical threats	Taxonomy review	Attention depletion, multitasking	N/A	Smart homes& IoT	Categorized riskfactors in behavioral SE
Arachchilage & Love (2014)	Security awareness	Survey-based	Low self-efficacy	Informing legalrisk allocation	Phishing	Users with low cybersecurity confidence fallprey more often

[13] National Cyber Security Centre (NCSC), *The psychology of cybersecurity: Understanding the human factor*, 2021, https://www.ncsc.gov.uk.

[14] R. Shillair *et al.*, „Online safety begins with you and me: Convincing Internet users to protect themselves", *Computers in Human Behavior,* 48/2015, 199–207.

[15] C. Hadnagy, *op. cit.*; European Union Agency for Cybersecurity (ENISA), *ENISA Threat Landscape 2022*, 2022, *https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022*, 20 April 2025.

Solove & Citron (2017)	Legal harm models	Legal theory	N/A	Advocates shared liability for cyber incidents	Cross-dom ain	Companies sharelegal responsibility for poor employee awareness
Brenner (2010)	Cybercrime definitions	Doctrinallegal analysis	N/A	Challenge of classifying SE as fraud	General SE	Difficulty prosecuting non-technical manipulation
Shillair *et al.* (2015)	Awareness campaigns	Mixed-method	Victim-blaming, self-efficacy	Legaland educational campaign design	Phishing	Education must incorporate empathy and behavioral science
NCSC (2021)	Policy implementation	Institutional guideline	Human-centered design	Security by design	National cybersecurity	Advocates for psychological ergonomics in software
ENISA (2022)	EU policy report	Threat-landscape analysis	N/A	Legal recognition of manipulation-based risks	Broad SE focus	Push for psychological awareness in cybersecurity laws
European Parliament (2016)	GDPR framework	Legal regulation	N/A	Outcome-based legal protection	Data breaches	GDPR lacks focuson behaviorally driven SE tactics

This review brought together and reviewed 72 peer-reviewed studies, 9 legal case analyses, and 11 institutional reports spanning the integration of behavioral science and cyber law.

The literature consistently brings forward the myriad cognitive problems that are commonly exploited in social engineering attacks. Trust heuristics, urgency cues, authority bias, and decision fatigue[16] are the most common ones. Phishing remains the most studied tactic, appearing in 63% of the behavioral studies reviewed, followed by Business Email Compromise (BEC) and pretexting scams. In workplace settings, trust manipulation proved especially effectives, where it is used to impersonate high-level executives.[17] High-stress environments were shown to jump up the susceptibility, with decision fatigue and cognitive overload linked to a 37% increase in user vulnerability to fraudulent links and communications.[18]

A key theme is that only 19% of the statutes and case law analyzed recognized manipulation-based attacks as distinct from conventional forms of fraud.

Most legal frameworks, including regulations like the GDPR, focus on addressing data breaches in terms of outcomes, with limited consideration for the behavioral mechanisms that enable such intrusions (General Data Protection

[16] D. Kahneman, *Thinking, fast and slow*, Farrar, Straus and Giroux, New York, 2011; K. Parsons *et al.*, "Predicting susceptibility to social influence in phishing emails", *International Journal of Human-Computer Studies,* 82/2015, 69–79.

[17] P. Kumaraguru, *op. cit.*, 7.

[18] R. F. Baumeister, *op. cit.*, 351–355.; R. Heartfield, G. Loukas, *op. cit.,* 398–428.

Regulation, GDPR). Despite these divides, there are efforts being made to align cybersafety measures with insights from behavioral science. Institutions such as the UK's National Cyber Security Centre (2021) and ENISA (2022) are promoting user-centered interventions—like warning nudges and phishing simulations—to help reduce human error.

5. CONCLUSION

This review voices a critical insight: the majority of cybersecurity breaches stem not from technical failings, but from psychological manipulation. Yet, legal frameworks have largely failed to evolve alongside these behavioral dynamics, often treating victims of cognitive exploitation no differently than those guilty of negligence.

To bridge this ever-increasing gap, there is a robust need to integrate behavioral science into both legal and cybersecurity policy frameworks. Doing so would enable more precise, equitable, and effective strategies for prevention and liability assessment.

Key recommendations include:

- Propagating behaviorally-informed awareness programs that move beyond generic training of compliance.
- Working on robust legal mechanisms that explicitly recognize cognitive manipulation as a distinct cybersecurity threat.
- Promoting interdisciplinary partnerships between legal experts, behavioral scientists, and cybersecurity practitioners.

Addressing the human factors at the core of social engineering is the need of the hour. It will be essential to build walls that are not only technically sound, but ethically and psychologically focused to the realities of modern cyber risk.

Please Note: The authors utilized AI-assisted tools to support the organization and synthesis of literature; most of the interpretations, critical evaluations, and conclusions reflect original scholarly analysis.

REFERENCES

Ajzen I., "The theory of planned behavior", *Organizational Behavior and Human Decision Processes,* 2/1991.

Arachchilage N. A. G., Love S., "Security awareness of computer users: A phishing threat avoidance perspective", *Computers in Human Behavior,* 38/2014.

Baumeister R. F., Vohs K. D., Tice D. M., "The strength model of self-control", *Current Directions in Psychological Science,* 6/2008.

Brenner S. W., *Cybercrime: Criminal threats from cyberspace*, Praeger, Santa Barbara – Denver – Oxford, 2010.

Hadnagy C., *Social engineering: The science of human hacking,* 2nd ed., Wiley, Indianapolis, 2018.

Heartfield R., Loukas G., „A taxonomy of cyber-physical threats and impact in the smart home", *Computers & Security,* 78/2016, 398–428.

Kahneman D., *Thinking, fast and slow*, Farrar, Straus and Giroux, New York, 2011.

Kumaraguru P. *et al.*, "Teaching Johnny not to fall for phish", *ACM Transactions on Internet Technology (TOIT),* 2/2009.

Kumar A., Bhatt M., Shukla R., "Human-centric cybersecurity: A review of social engineering attack detection and prevention", *Journal of Cybersecurity Technology,* 3/2021, 175–196.

Page M. J. *et al.*, "The PRISMA 2020 statement: An updated guideline for reporting systematic reviews", *BMJ,* 372, n71, 2021.

Parsons K. *et al.*, "Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)", *Computers & Security,* 42/2013.

Parsons K. *et al.*, "Predicting susceptibility to social influence in phishing emails", *International Journal of Human-Computer Studies,* 82/2015.

Rogers R. W., "Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation", *Social Psychophysiology* (eds. Cacioppo J., Petty R.), Guilford Press, New York, 1983.

Shillair R. *et al.*, "Online safety begins with you and me: Convincing Internet users to protect themselves", *Computers in Human Behavior,* 48/2015.

Solove D. J., Citron D. K., "Risk and anxiety: A theory of data-breach harms", *Texas Law Review,* 4/2017.

INTERNET SOURCES

European Union Agency for Cybersecurity (ENISA), *ENISA Threat Landscape 2022*, 2022, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

National Cyber Security Centre (NCSC), *The psychology of cybersecurity: Understanding the human factor*, 2021, https://www.ncsc.gov.uk

Verizon, *Data Breach Investigations Report 2023, https://www.verizon.com/business/resources/reports/dbir/*

LEGAL SOURCES

European Parliament, *Regulation (EU) 2016/679 of the European Parliament and of the Council.*

General Data Protection Regulation (GDPR), 2016, https://eur-lex.europa.eu/eli/reg/2016/679/oj

Monica Sahni, PhD*
Reva Kalra**

НАУКА О СОЦИЈАЛНОМ ИНЖЕЊЕРИНГУ: ПРАВНИ И БИХЕЈВИОРАЛНИ АСПЕКТ ПОДИЗАЊА СВЕСТИ О САЈБЕР БЕЗБЕДНОСТИ

Апстракт

Напади социјалног инжењеринга, који су одговорни за више од 80% успешних сајбер упада, користе људску психологију како би заобишли техничке заштите. Ово истраживање испитује основне бихејвиоралне механизме социјалног инжењеринга и њихове импликације на право и политику сајбер безбедности. Комбинујући психолошке експерименте са статистичким анализама фишинг напада и инцидената компромитовања пословне електронске поште (BEC), студија идентификује кључне когнитивне пристрасности, као што су манипулација поверењем и замор од доношења одлука, које нападачи користе. Поред тога, истраживање разматра улогу правних оквира у ублажавању ових напада, са фокусом на расподелу одговорности, спровођење прописа и заштиту жртава. Интеграцијом налаза из бихејвиоралних наука и правних студија, рад предлаже свеобухватни модел подизања свести о сајбер безбедности, наглашавајући циљану обуку, прилагодљив дизајн политика и сарадњу између јавног и приватног сектора. Овај приступ заснован на доказима има за циљ да смањи глобални утицај напада социјалног инжењеринга и допринесе обликовању будућих правних и едукативних стратегија.

Кључне речи: социјални инжењеринг, сајбер безбедност, фишинг, компромитовање пословне електронске поште (BEC), инциденти, заштита жртава.

* Истраживач, Jindal Global Law School, O. P. Jindal Global University, Сонепат, Индија, monicasahni@gmail.com.

** Истраживач, Sumona Institute of Behavioural Sciences and Performance Excellences, Њу Делхи, Индија.