ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

«Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ» КЕАҚ

Студенттер мен жас ғалымдардың
«ǴYLYM JÁNE BILIM - 2025»
XIX Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ
XX Международной научной конференции
студентов и молодых ученых
«ǴYLYM JÁNE BILIM - 2025»

PROCEEDINGS
of the XX International Scientific Conference
for students and young scholars
«ǴYLYM JÁNE BILIM - 2025»

2025
Астана

УДК 001(06)
ББК 72я631
F96

«ǴYLYM JÁNE BILIM – 2025» студенттер мен жас ғалымдардың XX Халықаралық ғылыми конференциясы = XX Международная научная конференция студентов и молодых ученых «ǴYLYM JÁNE BILIM – 2025» = The XX International Scientific Conference for students and young scholars «ǴYLYM JÁNE BILIM – 2025». – Астана: – 3813 б. - қазақша, орысша, ағылшынша.

ISBN 978-601-08-5373-7

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.В сборник вошли доклады студентов, магистрантов, докторантов имолодыхученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 001(06)
ББК 72я431
F96

ISBN 978-601-08-5373-7

Л.Н. Гумилев атындағы Еуразия ұлттық университеті, 2025

СЕКЦИЯ 2

СОВРЕМЕННЫЕ ИНФОРМАЦИОННЫЕ И КОММ УНИКАЦИОННЫЕ ТЕХНОЛОГИИ

Подсекция 2.2

Интеллектуальные информационные системы

255.	Сафонова Софья Александровна «Современные аспекты информационной безопасности в облачных вычислениях: модели, угрозы и методы защиты»	1034
256.	Смаилова Назгүл Батырбекқызы «Терең оқыту арқылы кітап ұсыныстарын әзірлеу: collaborative filtering, content-based және nlp әдістерінің комбинациясы»	1041
257.	Тажібай Аружан Айдосқызы, Кудубаева Сауле Альжановна «Көру қабілеті әлсіз адамдарға арналған аі дауыстық көмекші: нақты уақытта объектілерді анықтау және қашықтықты бағалау»	1046
258.	Тайжанов Азамат Жанкелдіұлы «Python тілінде фильмдердің интеллектуалды ұсыныс жүйесін әзірлеу»	1051
259.	Умирзахов Сундетали Кабылбекович «Сұраныстарды интеллектуалды талдау негізінде ұйымның сайты үшін чат-бот құру»	1055
260.	Шайхстан Марғұлан «IOT Сенсорлары негізінде ауа ластану деңгейін болжау»	1060

Подсекция 2.3

Современные тенденции в программной инженерии и управлении в условиях цифровой индустрии

261.	Bekenova A.B. «Development of a registration panel for users and doctors with integration into the database»	1077
262.	Bolat A.Zh. «Data analysis methods and decision making using big data and machine learning tools»	1081
263.	Алтайұлы А. «Visual studio интегралды ортасында «қойма қызметкерлеріне арналған» мәліметтер қорын жобалау»	1086
264.	Арап А.Қ. «Ақылды сурет салушы роботты әзірлеу»	1088
265.	Артыкбекқызы А. «Ақылды үйлердегі заттар интернеті(iot) мен робототехниканың өзара әрекеттесуі»	1091
266.	Ахметова А.Д. «Тоңазытқыштағы өнімдерді бақылауға және тағам әзірлеу ұсынысын беруге арналған программалық қосымша»	1096
267.	Дәрібай Д.Д. «Робототехниканы қолдану арқылы қойма логистикасындағы қолданыстағы басқару жүйелерін талдау»	1100
268.	Жамбулов С.Ж. «Білім алушыларды информатика және программалау олимпиадаларына дайындауда жасанды интеллекттің қолданысы»	1102
269.	Каиржан Р.С. «Development of system for recognition of emotional states of employees based on computer vision methods on Raspberry Pi»	1108
270.	Кайрекенова Н.Р. «Өнеркәсіптік роботты көру үшін машиналық оқытудың заманауи тәсілдері: әдістер, деректер жиынтығы және оптимизациялау»	1111

СЕКЦИЯ 3
ЕСТЕСТВЕННЫЕ НАУКИ

UDC 372.851.02

ANALYSIS OF SOCIAL ENGINEERING METHODS AND DEVELOPMENT OF A DEFENSE STRATEGY FOR CORPORATE STRUCTURES

Askhatov Alim
askhatov.alim@gmail.com
Department of Information Security System, Faculty of Information Technologies, Eurasian National University, Astana Kazakhstan
Supervisor – Z. Tashenova

1. Introduction

Social engineering has emerged as a primary corporate cyber threat, focusing on human psychology rather than technical vulnerabilities. Actors manipulate users through phishing, pretexting, baiting, and tailgating, leveraging psychological triggers like authority, urgency, reciprocity, and social proof to deceive employees into revealing sensitive information or granting access. This human-centered threat has grown rapidly – for example, phishing attack incidents have quadrupled since 2020, with more than one million incidents reported in one quarter of 2022. Notably, an estimated 78% of cyber incidents involve unintentional insider participation, which speaks to how employees tend to be the weakest security link.

Despite increasing awareness, traditional defenses that are purely technical in nature remain inadequate against these sophisticated social engineering methods. Attackers routinely bypass strong authentication or network defenses by exploiting humans (e.g. tricking users into divulging one-time passwords despite multi-factor authentication). To address these gaps, recent research by Askhatov et al. proposes a multi-layered defense strategy coupling technical safeguards, human-centered training, and organizational policy. This summary synthesizes the background, methodology, and primary findings of that research, with a focus on real-world deployment of the defense mechanisms and their impact. The goal is to provide cybersecurity practitioners with concise, actionable recommendations that effectively reduce social engineering risk.

2. Context and Methodology of the Study

The study first analyzed current social engineering methods and corporate weaknesses through a combination of literature review, case studies, and simulations. By examining real-world attack scenarios and psychological principles (e.g. Cialdini's influence principles of authority, scarcity, etc.), the authors extracted prevalent attack patterns and enabling human factors. Phishing emails, for instance, routinely instill urgency or fear of missing out to prompt rushed action, whereas impersonation exploits authority bias (e.g. posing as a CEO or IT admin) to bully compliance. This contextual analysis underscored the need for multi-faceted defenses addressing technology, people, and processes in tandem.

Methodologically, the researchers employed both qualitative and quantitative approaches. The authors used an LSTM-based model for detecting social engineering content, achieving high precision (0.89) and recall (0.87). They also tested a Q-learning-based incident response model, which improved reaction time by up to 19%.

The authors also simulated defense-response scenarios using reinforcement learning to optimize incident response strategies. They applied an enhanced Q-learning algorithm to adapt defenses in real time, which demonstrated 9–19% faster response times and more stable handling of varied attack sequences compared to baseline approaches. Throughout the research, findings were validated using statistical analysis and cross-validation (for models) to determine significance and generalizability. Finally, the study experimented with various defense mechanisms (technical tools, training, policies) in controlled corporate environments and real-case studies, measuring outcomes

such as phishing click-through rates, incident reporting frequency, and breach recovery time. These empirical experiments provided concrete evidence of which strategies yielded the most improvement, informing the recommended defense framework.

2.1 Multi-Layered Defense Strategies

A defense-in-depth model was developed from the analysis with the realization that no single solution is sufficient. The strategy combines three levels of defense – technical controls, human-centered programs, and organizational policy – to create a strong security posture. In this section, the actual implementation of measures in each category is delineated and their effectiveness is noted.

2.2 Technical Controls and Tools

Technical defenses are the frontline, operating to either detect or prevent social engineering attacks automatically from reaching end users. Some of the key tools used are:

- Phishing Detection Browser Extension – A custom browser extension was developed to detect and alert on suspicious websites and URLs in real time. It analyzes visited web pages for phishing red flags such as abnormal domain patterns, spoofed subdomains, or trigger words such as "verify" or "login". The extension also queries links against known phishing databases (e.g. PhishTank) for real-time threat intelligence. In initial testing, this tool effectively alerted users to phishing websites before they could engage, providing a valuable frontline defense for employees.
- Filtering and Spam Protection via Email – Next-gen email security gateways (e.g. Proofpoint, Mimecast) were introduced to filter out phishing emails. These offerings utilize content filtering and threat intelligence to quarantine ~80% of phishing emails prior to them even reaching user inboxes. Filtering lowers the risk an employee even sees a phishing lure by dramatically reducing the amount of malicious email.
- Multi-Factor Authentication (MFA) – Requiring MFA (via apps like Duo or Google Authenticator) adds a critical layer of account protection. Even if users are tricked into revealing passwords, MFA requires a second factor (token or biometric) to log in. Industry research and the case studies indicate MFA can prevent 50% or more of credential-based breaches by stopping attackers who have stolen passwords. In one deployment, enabling MFA for customers caused a 70% drop in account takeover incidents, drastically reducing phishing-based compromise.
- Anomaly Detection Systems – Machine learning-based anomaly detection (via tools like Splunk or Darktrace) actively monitors network and user behavior to detect abnormal patterns. The study's pilot deployment illustrated that anomaly detection alerts security teams to aberrant communication or login activity, reducing successful phishing intrusions by ~40% through early detection of suspicious activity. By identifying indicators of compromise (i.e. a sudden download of large amounts of data by an employee account at odd hours), these systems allow for a speedy response to presumed social engineering intrusions.
- Behavioral Profiling – Related to anomaly detection, some defenses build profiles of normal user behavior and communication patterns. Deviations from these norms (e.g., an employee receiving an email that doesn’t match standard sender profile or linguistic patterns) can be flagged for analysis. While more experimental, such profiling can be used to catch insider threats or targeted spear-phishing attacks that generic filters miss. In the comparative analysis, behavioral analytics were rated as moderately effective, with specific effectiveness in handling sophisticated or insider-focused social engineering scenarios.

Collectively, these technical controls provide an automated defense that makes social engineering attacks much less probable and minimizes their impact. They are preventive and detective controls that work best together – for example, using email filtering, anomaly detection, and MFA collectively provides overlapping defenses that an attacker would need to bypass simultaneously.

2.3 Human-Centric Security Measures

To strengthen the human factor, a combined program of gamified training, phishing simulations, and incentivized reporting was implemented. Gamified exercises and simulations reduced phishing click-through rates from 25% to as low as 8%, while feedback loops and reward systems increased incident reporting by 25%. These measures proved highly effective in developing user awareness and active participation in threat detection.

2.4 Organizational Policies and Preparedness

Organizational policies ensure that even if a social engineering attack succeeds, its impact is contained. Organizations with tested incident response plans recovered 40% faster. Regular security audits helped eliminate 15% of potential vulnerabilities. Role-Based Access Control (RBAC) reduced insider-related incidents by 30%, and improved physical access control cut unauthorized entries by 80%. These governance-focused practices ensure resilience, readiness, and accountability across teams.

3. Results and Effectiveness of the Defense Strategies

Empirical results from the case studies and simulations of the research demonstrate that a multi-layered approach can make a corporate structure substantially more resilient to social engineering.

On the technical side, the deployment of strong authentication and anomaly detection showed clear benefits. As noted, rolling out MFA to user accounts coincided with reductions of up to 70% in account takeover incidents, closing what had been a common result of phishing (stolen passwords leading to breaches). Likewise, pilot deployment of an AI-based anomaly detection system caught several spear-phishing attempts early, preventing damage and reducing overall incident levels by an estimated 40% compared with the pre-deployment period. These technical tool outcomes indicate that preventative controls can block a high percentage of social engineering attempts before they fool a human, especially when continuously refreshed with threat intelligence.

Human-centered defenses demonstrated perhaps the most immediate behavioral impact. Phishing simulation campaigns, when first initiated, would often register a high baseline click rate (e.g. 20–30% of employees fell for test phish initially). But over the period of several months of training and repeated simulations, organizations saw a steady reduction in click rates to single-digit percentages (as low as 5–8% in some divisions). Concurrently, the rate at which employees reported the simulated phishing emails rose dramatically, an indicator of heightened vigilance. Interestingly, departments that utilized the gamified training modules improved the most rapidly, an indicator of interactive training's effectiveness in altering behavior. Incentives increased reporting rates by 25%. This improved reporting is valuable because it gives security teams early warning to investigate actual phishing attacks before they spread.

Organizational measures provided priceless support during the study's observation time frame. Companies with refined incident response plans and who conducted regular drills contained mock breaches or actual incidents significantly better – cutting response times and recovery costs by a substantial margin (up to 40% faster recovery noted). Ongoing security audits not only patched policy gaps but served as a feedback loop to ensure technical and training measures remained effective against emerging threats. For example, when one phishing tactic using fake file-sharing links became popular, an audit triggered the updating of email filters to expressly warn of such unusual external share requests. This agility is a primary advantage of having formal governance and review established.

Combined, the multi-layered defense strategy reduced successful attack rates by up to 70%, improved employee phishing detection (click rates down to 5–8%), increased incident reporting by 25%, and shortened recovery times by up to 40%.

4. Conclusion

This overview lays out a comprehensive strategy for safeguarding corporate entities against the growing menace of social engineering. By incorporating technical controls (phishing detection software, anomaly monitoring, MFA, and email filtering), human-centered initiatives (continuous gamified training, phishing simulations, and incentives-based reporting), and sound organizational policies (incident response planning, security audits, and strict access controls), organizations can drastically reduce their vulnerability to social engineering attacks. The practical controls discussed – from a browser extension that intercepts phishing links in real time to an incentives program that rewards employees for reporting threats – have proven to offer value in actual use, bringing tangible improvement of security posture.

Most importantly, the findings demonstrate that a multi-layered defense-in-depth approach is far more effective than standalone initiatives. Cybersecurity professionals can take away not only specific actions (such as introducing MFA or conducting drills) but also the benefit of integrating these actions into a cohesive program. The benefits such as a 50–70% drop in successful attack rates, faster incident response, and enhanced user wariness attest to the real-world applicability of this approach in corporate environments. Going forward, organizations need to continuously update these measures – customizing training materials to new scams, refreshing tools with AI-driven enhancements, and reviewing policies against novel social engineering tactics. By doing this, businesses will develop an adaptive human-technology firewall, making it far more challenging for attackers to exploit the human element and ensuring that when they do try, the attempts are detected early and contained.

This article, based on Askhatov Alim's research work, is a sound evidence-based manual for practitioners. It argues that social engineering defense is not a single solution but an ongoing, integrated process. With strategic direction and determination on technical, human, and management levels, corporate entities can stay ahead of social engineers and protect their vital assets and information from manipulation-based intrusions.

Literature

1. D. N. Alharthi, M. M. Hammad, and A. C. Regan, “A taxonomy of social engineering defense mechanisms,” in *Advances in Intelligent Systems and Computing*, vol. 1130, pp. 17–29, 2020, doi: 10.1007/978-3-030-39442-4_2.
2. Al-Saraireh and A. Masarweh, “A novel approach for detecting advanced persistent threats,” *Egyptian Informatics J.*, vol. 23, no. 4, pp. 45–55, 2022, doi: 10.1016/j.eij.2022.06.005.
3. APWG, “Phishing Activity Trends Report, 2nd Quarter 2022,” Anti-Phishing Working Group, 2022.
4. C. I. Arimie and C. Onwubiko, “A framework for defending against social engineering attacks,” in *Proc. IEEE Eur. Symp. Security and Privacy Workshops (EuroS&PW)*, 2018, pp. 104–111, doi: 10.1109/EuroSPW.2018.00020.
5. Y. Aun, M. Gan, N. H. B. A. Wahab, and G. H. Guan, “Social engineering attack classifications on social media using deep learning,” *Computers, Materials & Continua*, vol. 74, no. 3, pp. 4917–4931, 2023, doi: 10.32604/cmc.2023.032373.
6. F. Breda, H. Barbosa, and T. Morais, “Social engineering and cyber security,” in *Proc. Int. Conf. Technology, Education and Development (INTED)*, Valencia, Spain, Mar. 2017, pp. 4204–4211, doi: 10.21125/inted.2017.1008.
7. I. Ghafir, V. Prenosil, A. Alhejailan, and M. Hammoudeh, “Social engineering attack strategies and defense approaches,” in *Proc. IEEE 4th Int. Conf. Future Internet of Things and Cloud (FiCloud)*, 2016, pp. 145–149, doi: 10.1109/FiCloud.2016.30.

8. I. Ghafir, V. Prenosil, and M. Hammoudeh, “A systematic review of social engineering attack strategies and defense mechanisms,” *Comput. Secur.*, vol. 68, pp. 208–227, 2017, doi: 10.1016/j.cose.2017.02.009.

9. C. Happ, A. Melzer, and G. Steffgen, “Trick with treat—reciprocity increases the willingness to communicate personal data,” *Comput. Hum. Behav.*, vol. 61, pp. 372–377, 2016, doi: 10.1016/j.chb.2016.03.051.

10. R. Heartfield and G. Loukas, “A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks,” *ACM Comput. Surv.*, vol. 48, no. 3, Art. 37, 2016, doi: 10.1145/2835375.

11. J. Hong, “The state of phishing attacks,” *Commun. ACM*, vol. 55, no. 1, pp. 74–81, 2012, doi: 10.1145/2063176.2063197.

12. M. Huber, S. Kowalski, and M. Nohlberg, “Towards automated social engineering: automatic generation of phishing emails,” *Comput. Secur.*, vol. 68, pp. 92–105, 2017, doi: 10.1016/j.cose.2016.12.007.

13. K. Krombholz, H. Hobel, M. Huber, and E. Weippl, “Advanced social engineering attacks and countermeasures,” *J. Inf. Secur. Appl.*, vol. 22, pp. 113–122, 2015, doi: 10.1016/j.jisa.2014.09.005.

14. K. D. Mitnick and W. L. Simon, *The Art of Deception: Controlling the Human Element of Security*. Indianapolis, IN, USA: Wiley, 2002.

15. F. Mouton, M. M. Malan, L. Leenen, and H. S. Venter, “Social engineering attack framework,” in *Proc. Information Security for South Africa (ISSA)*, Johannesburg, South Africa, 2016, pp. 1–8, doi: 10.1109/ISSA.2016.7802920.

16. C. I. Nwakanma and C. N. Chukwunweike, “Social engineering attacks in the digital age,” *J. Cybersecurity Res.*, vol. 10, no. 1, pp. 34–50, 2018, doi: 10.21125/inted.2017.1008.

17. K. Parsons, D. Calic, M. Pattinson, M. Butavicius, A. McCormac, and T. Zwaans, “The human aspects of information security questionnaire (HAIS-Q): two further validation studies,” *Comput. Secur.*, vol. 66, pp. 40–51, 2017, doi: 10.1016/j.cose.2017.01.004.

18. G. Potamos, S. Theodoulou, E. Stavrou, and S. Stavrou, “Building maritime cybersecurity capacity against ransomware attacks,” in *Cybersecurity, Situational Awareness and Social Media*, Singapore: Springer, 2023, pp. 87–101, doi: 10.1007/978-981-19-6414-5_6.

19. F. Salahdine and N. Kaabouch, “Social engineering attacks: a survey,” *Future Internet*, vol. 11, no. 4, p. 89, 2019, doi: 10.3390/fi11040089.

20. P. Schaab, K. Beckers, and S. Pape, “Social engineering defence mechanisms and counteracting training strategies,” *Inf. Comput. Secur.*, vol. 25, no. 2, pp. 206–222, 2017, doi: 10.1108/ICS-04-2017-0022.

21. H. Siadati, T. Nguyen, P. Gupta, M. Jakobsson, and N. Memon, “Mind your SMSes: mitigating social engineering in second factor authentication,” *Comput. Secur.*, vol. 65, pp. 14–28, 2017, doi: 10.1016/j.cose.2016.11.009.

22. F. Stajano and P. Wilson, “Understanding scam victims: seven principles for systems security,” *Commun. ACM*, vol. 54, no. 3, pp. 70–75, 2011, doi: 10.1145/1897852.1897872.

23. K. Thomas et al., “Data breaches, phishing, or malware? Understanding the risks of stolen credentials,” in *Proc. 2017 ACM SIGSAC Conf. Comput. Commun. Secur. (CCS)*, 2017, pp. 1421–1434, doi: 10.1145/3133956.3133996.

24. Verizon, “2022 Data Breach Investigations Report,” Verizon Enterprise, 2022.

25. C. Yang, Y. Chen, and M. Tang, “A novel approach to detecting social engineering attacks using machine learning,” *J. Cybersecurity*, vol. 9, no. 1, pp. 35–50, 2021, doi: 10.1093/cybsec/tyaa018