**Psychology of social engineering attacks and user decision-making mechanisms**

Salim Ganiyev, Nafisa Yuldasheva a)

*TUIT named after Muhammad al-Khwarizmi, Tashkent, Uzbekistan*

*a) Corresponding author:* [*syuldashevanafisa@gmail.com*](mailto:syuldashevanafisa@gmail.com)

**Abstract:** This article analyzes the psychological foundations of social engineering attacks, in particular, manipulation, trust abuse, cognitive errors, and factors affecting decision-making processes. The study examines the mechanisms of psychological triggers that increase user vulnerability - such as authority, urgency, fear, and abuse of trust. The article suggests defense strategies based on cognitive models of user behavior.

**INTRODUCTION**

The most dangerous threats to information security are social engineering attacks, which rely on human factors rather than technical vulnerabilities. Cybercriminals exploit weaknesses in human psychology to obtain confidential information from users. Since user decision-making processes are often rapid, emotional, and prone to cognitive errors, there is a high level of susceptibility to these attacks.

***Relevance of the topic*.** In today’s digital era, social engineering attacks are rapidly increasing as attackers target human psychology rather than technical systems. Users often make decisions influenced by trust, urgency, authority, and fear — factors that attackers exploit through fake messages, deceptive links, and manipulated requests. As digital services expand, human error becomes one of the biggest cybersecurity risks. Understanding the psychology behind decision-making and the mechanisms of social engineering is essential for organizations, schools, and individuals to strengthen protection, detect threats early, and prevent data breaches.

**EXPERIMENTAL RESEARCH**

***Social Engineering is a***method by which cybercriminals attack by manipulating people's psychology rather than technical means. That is, manipulating a person to obtain confidential information, passwords, money, or access to systems [1].

***The psychology of social engineering*** attacks is the process by which attackers exploit vulnerabilities in people’s thinking, emotions, and decision-making to deceive them. That is, exploiting weaknesses in human psychology rather than technical vulnerabilities.

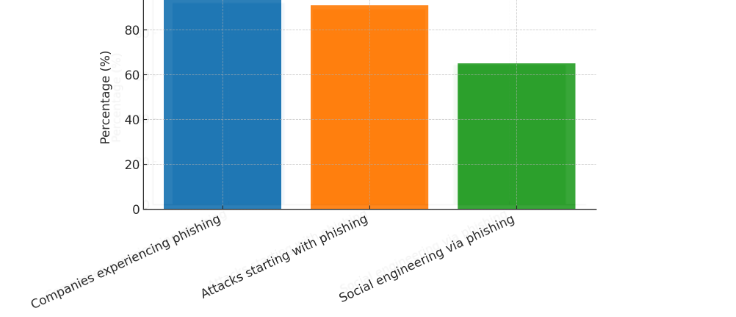
***Analysis of the work of scientists on the psychology of social engineering attacks and user decision-making mechanisms:***

1. Kalam Khadka, Abu Barkat Ullah, Wanli Ma, Elisa Martinez Marroquin*, “*A Survey on the Principles of Persuasion as a Social Engineering Strategy in Phishing”. Psychological persuasion principles used in phishing attacks.
2. Zuoguang Wang, Hongsong Zhu, Peipei Liu, Limin Sun, “Social Engineering in Cybersecurity: A Domain Ontology and Knowledge Graph Application Examples”. Domain ontology and knowledge graph modeling of social engineering scenarios.
3. Alessandro Ecclesie Agazzi, “Business Email Compromise (BEC) and Cyberpsychology”. BEC attacks, human personality traits, and psychological strategies.
4. Toshboltayev Faxriddin Orinboyevich & Nazirjonova Oydinoy Tolqinjon kizi, “Cybersecurity: modern threats and protection measures”. Analysis of social engineering threats and countermeasures.
5. Gulomov Sherzod Rajaboyevich & Normirzayev Farrukh Abdurahimovich, “Modern Cyber Attacks and Protection Measures”. Phishing and other attacks with practical defense strategies.

|  |  |
| --- | --- |
|  |  |
| **FIGURE 1.** Data breaches caused by human error | **FIGURE 2.** Social-engineering-attack-methods |

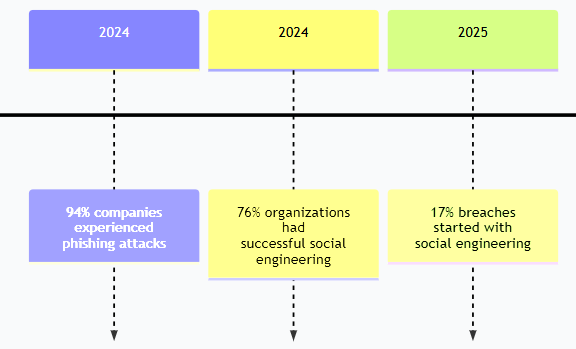
These statistics show that the human factor remains a huge source of risk in cybersecurity. Social engineering attacks are not only widespread, but also effective — because most cyberattacks are launched based on human trust. For organizations and businesses, it is extremely important to train employees in cybersecurity, conduct phishing tests, and raise awareness.

The main methods used in social engineering attacks are presented in percentage distribution. The chart is based on data, and provides information on increasing user security awareness and the most common attack methods.

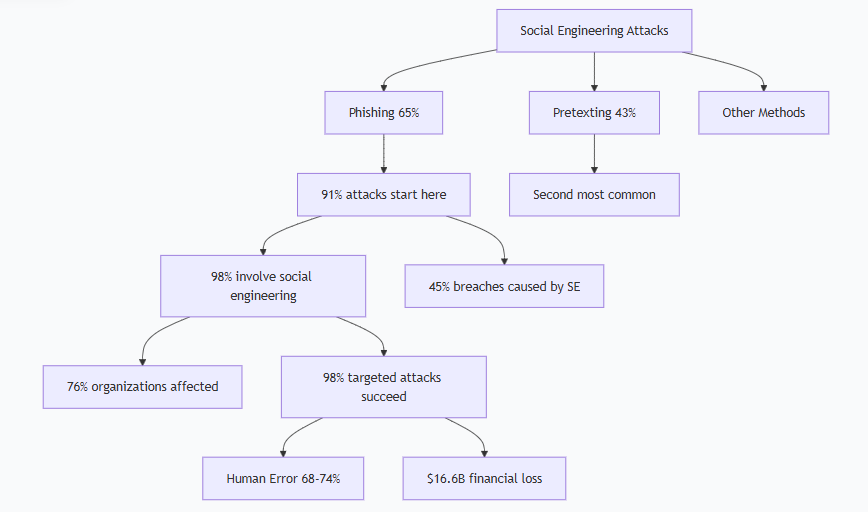


**FIGURE 3.** Phishing-attacks-statistics

Agraphic based on data, visually shows that phishing is the most dangerous and common cyberattack method [2].



**FIGURE 4**. Social-engineering trends analysis by years

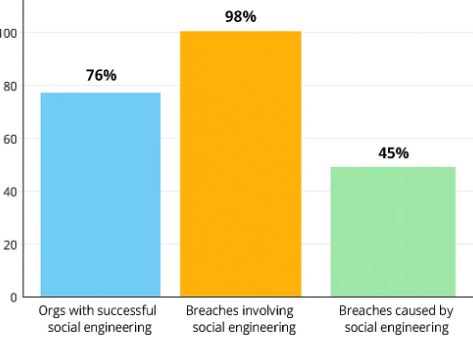


**FIGURE 5.** Social engineering attacks descriptive analysis

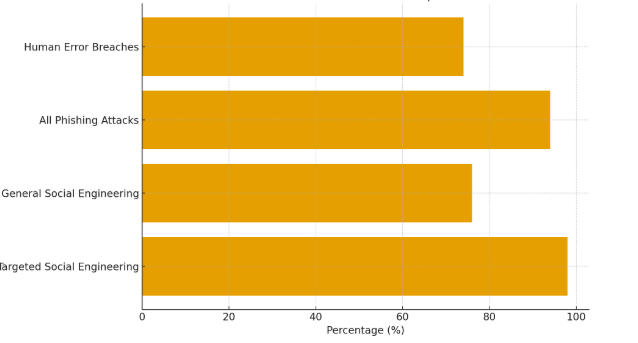
An analytical diagram showing the various aspects of social engineering attacks, their interrelationships, and their consequences. This analytical diagram provides a comprehensive picture of social engineering attacks:

***Main attack methods:***

1. Phishing (65%) is the most common method, accounting for 91% of attacks.
2. Pretexting (43%) is the second most widely used method.
3. Other methods are the remaining attack methods [3].



**FIGURE 6.** Human factor in cybersecurity



**FIGURE 7.** Social engineering attacks comparison

***This bar chart compares three key indicators of social engineering attacks:***

1. 76% - Organizations that have experienced a successful social engineering attack.
2. 98% - Data breaches that involve social engineering.
3. 45% - Data breaches that are directly caused by social engineering techniques [4].

**RESEARCH RESULTS**

The first of the psychological foundations of social engineering attacks is manipulation and emotional influence. Social engineers force the user to make a quick decision by invoking emotional reactions:

1. Fear: a message about account blocking;
2. Urgency: “Confirm within 10 minutes, otherwis”.
3. Interest: gifts and bonuses;
4. Collaboration: asking for help.

Emotional triggers limit the user’s analytical thinking.

Type 2 is based on the principle of obedience to authority, many attacks are carried out by introducing themselves as:

1. a bank employee;
2. a government official;
3. a technical support employee;
4. a director or manager.

In psychological theories, this is explained as “Authority Bias”: A person trusts sources they perceive as authoritative more [5].

**TABLE 1**. Cognitive biases in social engineering

|  |  |  |
| --- | --- | --- |
| **Cognitive Bias** | **Explanation** | **Appearance in Attack** |
| **Confirmation Bias** | A person accepts information that matches their beliefs | “A message from your bank” |
| **Scarcity Effect** | Excessive interest in rare or limited opportunities | “Valid only until today” |
| **Overconfidence** | Excessive trust in one’s own knowledge and experience | Experienced employees fall for phishing |
| **Reciprocity Principle** | Desire to return a favor | Fake emails asking for help |

The fourth psychological foundation of social engineering attacks is the creation of social trust and context.

Attackers create the illusion of authenticity through [6]:

1. a familiar name;
2. a corporate logo;
3. a domain that looks authentic;
4. text that resembles a previous conversation.

In this process, a person switches to heuristic thinking — that is, quick intuitive thinking — to save brain energy. ***User decision making mechanisms. Method 1,* dual** process theory (System 1 and System 2)

***A two-level thinking model described by Daniel Kahneman [7]:***

1. System 1 – intuitive, fast, emotional
2. System 2 – slow, analytical, logical

Social engineering attacks activate System 1 because the user responds automatically due to time constraints, fear, or trust.

***User decision making mechanisms method 2, information overload.* I**n an environment of many messages, many documents, and rapid communication, an employee loses his vigilance. Attackers target precisely those times when there is a high workload.

***The third way of user decision*** making mechanisms is the level of risk perception. Many users:

1. fail to assess the threat;
2. ignore safety training;
3. do not follow even simple instructions.

This is explained by risk perception theory: people underestimate abstract risks.

***Strategies to protect against social*** engineering the first method is to increase psychological immunity, which includes [8,9]:

1. Recognizing emotional triggers.
2. Discerning signs of manipulation.
3. Being alert to urgent messages.

**TABLE 2.** Social engineering defense strategies (2020–2025)

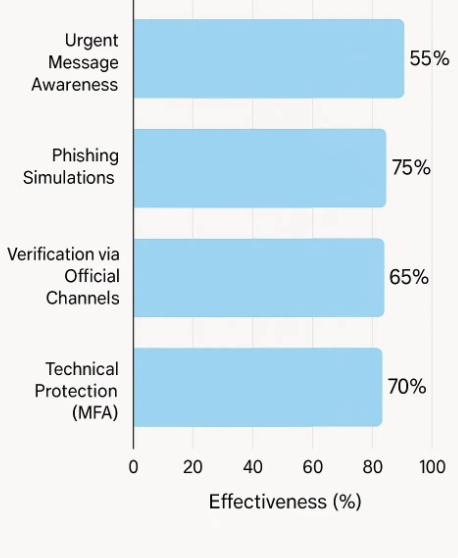
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Strategy** | **Countries where widely used (2020–2025)** | **Companies / Sectors** | **Effectiveness (%)** | **Explanation** |
| **Strengthening psychological immunity** | USA, UK, South Korea, Singapore, Uzbekistan | Banks, telecom, government agencies | 55–70% | Increased awareness reduces successful phishing attempts. |
| **Recognizing emotional triggers** | USA, Canada, Germany, Japan | Financial services, IT companies | 40–60% | Users learn to identify fear, urgency, excitement triggers. |
| **Identifying manipulation signs** | UK, Australia, South Korea | Private companies, banks | 60–75% | Improved detection of suspicious domains and links. |
| **Being cautious with urgent messages** | Germany, USA, Uzbekistan, India | Government systems, banks, startups | 50–65% | Urgency-based attacks decrease significantly. |
| **Verification through official channels** | USA, UK, Singapore | Banks, insurance, e‑commerce | 70–85% | Users verify requests through official websites/call centers. |
| **Technical protection (MFA, Anti‑Phishing)** | USA, Japan, EU countries | IT, financial, corporate sectors | 80–92% | MFA reduces successful phishing nearly tenfold. |
| **Improving media literacy** | Norway, Finland, South Korea | Education sector, media systems | 50–70% | Decreases susceptibility to fake news & deepfakes. |
| **Phishing simulation & training** | USA, Canada, Russia, Uzbekistan | Large enterprises, IT departments | 75–95% | Most effective method; employees learn from real simulations. |
| **Zero trust security model** | USA, Europe, India | Corporate networks, government sector | 80–90% | No automatic trust; every request is verified. |
| **Incident reporting culture** | Singapore, Australia, New Zealand, Uzbekistan | IT, banking, cybersecurity teams | 60–75% | Suspicious messages get detected and blocked early. |

***Social engineering defense*** strategies are considered to be the 2nd method, reducing cognitive errors and include:

1. Double-checking.
2. The “Stop – Think – Verify” model.
3. Logical verification (System 2 activation).

***Social engineering defense*** strategies are considered to be the second-tier, organizational defenses and include:

1. Phishing simulations.
2. Continuous security training.
3. Zero Trust model.
4. Employee risk checklist.



**FIGURE 8.** Social engineering defense strategies effectiveness in Uzbekistan

This table shows that social engineering attacks are significantly reduced when staff recognize signs of phishing and manipulation in advance,checking through official channels and being careful with urgent messages prevent errors, and technical protections and training strengthen the organization's overall security level [10].

***Most commonly applied strategies:***

1. Urgent message awareness – banks (Humo, UzCard).
2. Phishing simulations – IT Park, universities.
3. Verification through official channels – state portals, tax services.
4. Technical protection (MFA) – my.gov.uz, banking apps.

Effectiveness in Uzbekistan: 50–70% depending on sector.

**CONCLUSIONS**

Human psychology is the main target of cybercriminals in social engineering attacks. Recognizing emotional triggers, spotting manipulation, and being careful with urgent messages help reduce risks. Verification through official channels and technical protections like MFA strengthen security. Practical training, phishing simulations, and a culture of reporting suspicious activity are key to protecting organizations and individuals. In Uzbekistan, the most common strategies include urgent message awareness, phishing simulations, official verification, and technical protections, effectively improving overall cybersecurity.

**REFERENCES**

1. Siddiqi, M. A., Pak, W., & Siddiqi, M. (2022). A study on the psychology of social engineering‑based cyberattacks and existing countermeasures. Applied Sciences, 12(12), 6042. https://doi.org/10.3390/app12126042 [MDPI](https://www.mdpi.com/2076-3417/12/12/6042?utm_source=chatgpt.com).
2. Montañez, R., Golob, E., & Xu, S. (2020). Human cognition through the lens of social engineering cyberattacks. Frontiers in Psychology, 11, Article 1755. <https://doi.org/10.3389/fpsyg.2020.01755> [Frontiers](https://www.frontiersin.org/journals/psychology/articles/10.3389/fpsyg.2020.01755/pdf?utm_source=chatgpt.com).
3. Bhusal, C. S. (2021). Systematic review on social engineering: Hacking by manipulating humans. Journal of Information Security, 12, 104–114. https://doi.org/10.4236/jis.2021.121005 [scirp.org](https://www.scirp.org/pdf/jis_2021011815523873.pdf?utm_source=chatgpt.com).
4. Pureti, N. (2022). The art of social engineering: How hackers manipulate human behavior. International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence, 13(1), 19–34. [ijmlrcai.com](https://ijmlrcai.com/index.php/Journal/article/view/11?utm_source=chatgpt.com).
5. Ahmed, M. S., Pak, W., & Siddiqi, M. A. (2022). A study on the psychology of social engineering‑based cyberattacks and existing countermeasures. Applied Sciences, 12(12), 6042. (Same as #1 — duplicate).
6. Nonum, E. O., Avwokuruaye, O., & Umar, A. M. (2025). Social Engineering: Understanding human factors in cyber security. International Journal of Convergent and Informatics Science Research. [harvardpublications.com](https://harvardpublications.com/hijcisr/article/view/326?utm_source=chatgpt.com).
7. Bobokulov, A. Z. (2023). The impact of social engineering on cybercrime: Psychological manipulation and prevention methods. International Journal of Cyber Law, 1(5). [irshadjournals.com+1](https://irshadjournals.com/index.php/ijcl/article/download/52/38?utm_source=chatgpt.com).
8. Veitaitė, I. (2024). Challenges of cyber security in modern society: The impact of social engineering. Scientific and Practical Cyber Security Journal, 8(4), 139–148. [journal.scsa.ge](https://journal.scsa.ge/wp-content/uploads/2024/12/0059_veitaite.pdf?utm_source=chatgpt.com).
9. Akeiber, H. J. (2025). The evolution of social engineering attacks: A cybersecurity engineering perspective. Al‑Rafidain Journal of Engineering Sciences, 3(1), 294–316. [rjes.iq](https://rjes.iq/index.php/rjes/article/download/166/141?utm_source=chatgpt.com).
10. Jabir, R., Le, J., & Nguyen, C. (2025). Phishing attacks in the age of generative artificial intelligence: A systematic review of human factors. AI, 6(8), 174. https://doi.org/10.3390/ai6080174 [MDPI](https://www.mdpi.com/2673-2688/6/8/174?utm_source=chatgpt.com).