Yuzhalin Oleg Pavlovich
student
Fedorov Daniil Emilevich
student
Scientific supervisor
Vrublevsky Yuri Olegovich
Senior lecturer
RTU MIREA
Moscow

ASSESSMENT OF ECONOMIC RISKS CAUSED BY LINGUISTIC MANIPULATION IN ENGLISH-LANGUAGE PHISHING ATTACKS ON THE FINANCIAL SECTOR

Abstract*: the article analyzes economic risks arising from English-language phishing attacks aimed at financial institutions. Special attention is paid to linguistic manipulation as a key mechanism of social engineering that influences user behavior. The research examines typical linguistic patterns used in phishing messages and evaluates their impact on direct and indirect financial losses. The methodological basis of the study includes analysis of academic literature, industry reports, and concepts from behavioral economics and cognitive psychology. The results indicate that linguistic manipulation significantly increases the effectiveness of phishing attacks by exploiting cognitive biases and reducing critical perception. The conclusions may be applied in the development of risk assessment models and preventive cybersecurity measures in the financial sector.*

Keywords*: phishing, economic risk, linguistic manipulation, financial sector, cybersecurity, social engineering.*

Южалин Олег Павлович
студент
Фёдоров Даниил Эмильевич
студент

Научный руководитель

Врублевский Юрий Олегович

старший преподаватель

ФГБОУ ВО «МИРЭА – Российский технологический университет»

г. Москва

ОЦЕНКА ЭКОНОМИЧЕСКИХ РИСКОВ, ВЫЗВАННЫХ ЛИНГВИСТИЧЕСКИМИ МАНИПУЛЯЦИЯМИ В АНГЛОЯЗЫЧНЫХ ФИШИНГОВЫХ АТАКАХ НА ФИНАНСОВЫЙ СЕКТОР

Аннотация*: в статье анализируются экономические риски, связанные с англоязычными фишинговыми атаками, направленными на финансовые учреждения. Особое внимание уделяется лингвистической манипуляции как ключевому механизму социальной инженерии, влияющему на поведение пользователей. В исследовании рассматриваются типичные лингвистические шаблоны, используемые в фишинговых сообщениях, и оценивается их влияние на прямые и косвенные финансовые потери. Методологическая основа исследования включает анализ научной литературы, отраслевых отчетов и концепций поведенческой экономики и когнитивной психологии. Результаты показывают, что лингвистические манипуляции значительно повышают эффективность фишинговых атак за счет использования когнитивных искажений и снижения критического восприятия. Выводы могут быть использованы при разработке моделей оценки рисков и превентивных мер кибербезопасности в финансовом секторе.*

Ключевые слова*: фишинг, экономический риск, лингвистические манипуляции, финансовый сектор, кибербезопасность, социальная инженерия.*

The ongoing digitalization of the financial sector has fundamentally transformed the way financial services are delivered. Online banking, electronic payment systems, and mobile financial applications have become an integral part of everyday life. At the same time, the growing dependence on digital technologies has led to an increase in cyber threats, among which phishing attacks occupy a central position. Phishing represents a form of cybercrime that relies primarily on psychological and linguistic influence rather than technical exploitation of information systems.

In addition to direct financial damage, phishing attacks create hidden economic costs that are often underestimated. Financial institutions are required to allocate significant resources to internal investigations, forensic analysis, and system audits after an incident. These activities divert personnel and financial resources away from core business operations, reducing overall productivity. Over time, repeated phishing incidents may increase operational inefficiency and negatively affect financial performance.

Another important factor is the impact of phishing on customer behavior. Users who have experienced or observed phishing incidents tend to reduce their use of digital financial services or demand additional security guarantees. This behavior limits the adoption of innovative financial technologies and slows digital transformation. From an economic standpoint, reduced service usage leads to lower transaction volumes and diminished revenue growth for financial institutions.

Moreover, linguistic manipulation complicates legal and regulatory response mechanisms. Phishing messages often operate in a gray area where intent is difficult to prove due to indirect language and social engineering techniques. This increases legal uncertainty and raises compliance costs, as financial organizations must invest in monitoring, documentation, and reporting procedures to meet regulatory requirements.

Financial institutions are particularly attractive targets for phishing attacks due to the direct access to monetary assets and sensitive customer data. Economic damage caused by phishing is not limited to immediate financial losses resulting from unauthorized transactions. In many cases, financial organizations are forced to compensate affected clients, which increases operational expenses. In addition, phishing incidents often lead to reputational damage, loss of customer trust, and increased regulatory scrutiny, all of which have long-term economic consequences.

From an economic perspective, phishing attacks generate both direct and indirect risks. Direct risks include theft of funds, fraudulent payments, and costs associated with incident response. Indirect risks involve reputational losses, legal expenses, regulatory fines, and the need for additional investments in cybersecurity infrastructure. Studies in the economics of information security emphasize that indirect losses may exceed direct financial damage over time, especially in the financial sector where trust plays a crucial role.

A key factor contributing to the success of phishing attacks is linguistic manipulation. English-language phishing messages are often designed to imitate official communication from banks, payment systems, or financial regulators. The use of formal vocabulary, professional tone, and standardized structures increases the perceived legitimacy of such messages. In addition, attackers frequently employ urgency cues, such as warnings about account suspension or suspicious activity, in order to create psychological pressure and reduce critical thinking.

Emotional manipulation is another important linguistic strategy used in phishing campaigns. Messages may appeal to fear of financial loss, concern for account security, or expectation of financial gain. These emotional triggers activate cognitive biases described in behavioral economics, including loss aversion and authority bias. As a result, users are more likely to comply with the instructions contained in phishing messages without verifying their authenticity.

Cognitive psychology provides a useful framework for understanding why linguistic manipulation is effective. According to dual-process theories of thinking, human decision-making operates through two systems: a fast, intuitive system and a slow, analytical system. Phishing messages are specifically designed to activate intuitive responses and bypass analytical reasoning. Time pressure, emotional language, and perceived authority all contribute to this effect.

In the financial context, the consequences of such cognitive manipulation are particularly severe. Financial decisions often involve sensitive information and irreversible transactions. A single successful phishing attack can lead to significant economic losses for both individual users and financial institutions. Moreover, large-scale phishing campaigns may undermine public confidence in digital financial services, creating systemic risks for the financial sector.

Effective mitigation of economic risks associated with phishing requires an interdisciplinary approach. Technical security measures, such as email filtering and authentication protocols, remain essential but are not sufficient on their own. Linguistic analysis of suspicious messages can enhance phishing detection systems by identifying manipulative language patterns. Such an approach allows organizations to reduce the probability of successful attacks and, consequently, expected economic losses.

Education and awareness programs also play a crucial role in risk reduction. Training employees and customers to recognize linguistic manipulation techniques can significantly decrease susceptibility to phishing. From an economic standpoint, investments in preventive measures are generally more cost-effective than expenditures related to incident response and recovery. Therefore, incorporating linguistic and behavioral factors into cybersecurity strategies is an important step toward improving the overall economic resilience of the financial sector.

References

1. Anderson R.W. [et al.]. Measuring and Managing the Economics of Cyber Security.

2. Gordon L.A., Loeb M.P. The Economics of Information Security: A Strategic and Practical Perspective.

3. Ponemon Institute. Cost of a Data Breach Report.

4. Bauer J.M., van Eeten M.J.G. Cybersecurity: Economic and Social Perspectives.

5. Cialdini R.B. Influence: The Psychology of Persuasion.

6. Shneier B. Secrets and Lies: Digital Security in a Networked World.

7. Kahneman D. Thinking, Fast and Slow.

8. Industry reports by Microsoft, Cisco, and Trend Micro.