Pakistan Journal of Life and Social Sciences
www.pjlss.edu.pk

https://doi.org/10.57239/PJLSS-2026-24.1.0042

RESEARCH ARTICLE

Socio-Technical Approach to Teaching Employees How to Counter Phishing Attacks: Architecture of a System with Behavioral Monitoring and Adaptive Learning

Svetlana Belikova[1*], Natalia Yazvinskaya[2*]

[1,2] Don State Technical University, Rostov-on-Don, Russia

ARTICLE INFO

Received: APR 15, 2026

Accepted: MAY 5, 2026

Keywords

Phishing
Human Factor
Activity Monitoring
Adaptive Learning
Sociotechnical Systems
Information Security
Behavioral Analysis
Social Engineering

***Corresponding Author:**
lionnat@mail.ru

ABSTRACT

The article discusses the problem of increasing the vulnerability of corporate information systems to phishing attacks through the human factor, which, according to research, becomes the cause of most successful incidents. An integral sociotechnical approach is proposed, combining technical monitoring of user activity with sociological analysis of organizational roles and behavioral patterns of employees. The architecture of the software system has been developed. The system includes modules for generating personalized phishing scenarios, monitoring behavioral responses, and adaptive learning, which allows for the creation of individual learning paths based on employees' professional profiles. According to the users' affiliation with a particular socio-professional group, the developed modular system adapts the complexity and content of the training materials, as well as allows for the generation of personalized phishing scenarios.

INTRODUCTION

In today's digital economy, information assets are becoming a key resource for organizations. Paradoxically, despite advances in technical security, the effectiveness of cyberattacks is not declining, but rather increasing. Attacks are becoming increasingly sophisticated, and social engineering methods are increasingly being used to implement them. Phishing, as a social engineering method aimed at exploiting the human factor, continues to demonstrate a steady increase in the share of all cybercrimes. Based on an analysis of modern research (including data from Elevate Security), it has been revealed that 4% of employees are responsible for 92% of successful incidents, with mid-level managers being the most vulnerable . According to the Verizon Data Breach Investigations Report (2023), 68% of information leaks are based on the use of various social engineering methods [1]. Moreover, the technical complexity of attacks is often inferior to their psychological sophistication. The traditional approach to information security has viewed humans primarily as the "weak link" in the security perimeter. However, modern research shows that this model is incomplete. The human factor should not be viewed as a static vulnerability, but as a dynamic component of the system, influenced by organizational, social, and individual factors.

This requires a shift in focus from purely technical barriers to systemic employee training, corporate culture transformation, and the implementation of solutions that proactively prevent human error. The software developed in this study serves as a practical tool for such a transformation, implementing targeted training for vulnerable groups through personalized phishing simulations and developing sustainable behavioral norms through a continuous cycle of

testing, feedback, and adjustment. This approach not only reduces the rate of successful attacks but also creates a qualitatively new, conscious information security environment within the organization.

The goal of this work is to develop a software system architecture that combines technological monitoring and learning capabilities with a sociological understanding of vulnerability factors in an organizational context.

To achieve the stated research goal—developing a software tool for training and monitoring user activity in the context of phishing threats—the following key objectives were identified: conducting an in-depth analysis of sociological factors (such as organizational roles, corporate culture, and communication patterns) that determine employee susceptibility to phishing in the corporate environment; based on this analysis, developing a user profiling model that integrates their socio-professional characteristics and behavioral patterns to personalize the training impact; designing a system architecture that seamlessly combines modules for generating training phishing scenarios, monitoring user behavioral responses in real time, and implementing adaptive learning trajectories based on profiling data.

Sociological Analysis of Phishing Susceptibility Factors in the Corporate Environment

Theoretical and Methodological Foundations of Human Factor Research in Cyber Security

The traditional engineering-technical approach to information security, which long dominated academic and corporate environments, viewed humans primarily as the "weak link" in the security perimeter—a source of uncontrolled errors and deviations from regulations [2]. However, accumulated empirical data demonstrate a stable correlation between the success of phishing attacks and a wide range of social, organizational, and role-based characteristics of employees. This necessitates a paradigm shift: from perceiving the human factor as statistical noise to conceptualizing it as a complex, structurally conditioned social phenomenon requiring in-depth sociological analysis.

In the present study, susceptibility to phishing is examined not as a purely individual psychological trait (gullibility, inattention, low digital literacy) but as a socially constructed behavioral pattern shaped by three groups of factors: institutional-role factors (the employee’s position in the organizational hierarchy and associated role expectations), sociocultural factors (norms, values, and informal practices within the work collective), and communicative factors (the specifics of information flows, interaction channels, and data exchange protocols).

A key factor differentiating the level of vulnerability to phishing attacks is the employee’s professional and job position. The statistics [1] point not to random individual errors but to the existence of stable "risk groups" formed by the very structure of the organization.

Middle managers demonstrate the greatest vulnerability. This group occupies a structurally complex position: while endowed with significant autonomy in operational decision-making and broad access rights to financial and personnel information, they are simultaneously situated within intensive information flows between the strategic level (senior management) and the execution level (rank-and-file specialists). This generates specific role demands: the need to respond quickly to a high volume of incoming requests, often coming from external counterparties, and simultaneously, the absence of institutionalized filtering of correspondence (unlike senior management, who delegate this function to assistants and secretariats). Thus, the role-based vulnerability of middle managers is not a consequence of personal incompetence but an immanent property of their position within the organizational structure.

In contrast, senior management exhibits lower success rates for phishing attacks, which is explained not so much by higher qualifications as by organizational protection: the presence of administrative barriers (assistants, referents) that mediate their direct interaction with the digital environment. Rank-and-file employees, in turn, although lacking such developed administrative protection, possess fewer critical access rights, which reduces the attractiveness of this group as a target for targeted attacks.

A second significant factor determining susceptibility to phishing is the type of corporate culture. Using the typology of K. Cameron and R. Quinn (Competing Values Framework) [3], stable correlations can be identified between an organization's cultural models and specific vulnerabilities to social engineering attacks (Table 1).

Table 1: Correlation of organizational factors with vulnerability to phishing

Organizational factor	Mechanism of influence on vulnerability	Type of phishing attack
Degree of centralization of decision-making	High centralization → rapid execution of "management orders" without verification	CEO-fraud, Business Email Compromise
Intensity of external communications	Frequent document exchange with counterparties → reduced vigilance regarding attachments	Mass phishing with malicious attachments
Level of digitalization of processes	High digitalization → more entry points for attacks, habit of automation	Phishing via corporate messengers, fake portals
Corporate culture (according to K. Cameron and R. Quinn)	Clan culture (high trust) → vulnerability to personalized "from a colleague" attacks	Targeted spear-phishing, messenger compromise

In organizations dominated by a hierarchical culture, oriented toward strict adherence to regulations and vertical communications, CEO-fraud class attacks (attacks using forged corporate emails purportedly from senior management) are characterized by elevated risk. Employees accustomed to unquestioningly following orders from superiors, under time pressure or when faced with the external trappings of an official request, tend to ignore verification protocols.

A modern business culture oriented toward results and competition produces a different vulnerability: a tendency toward prompt interaction with counterparties and partners at the expense of thorough verification [4]. Under such conditions, attacks that mimic urgent commercial offers or requests from key clients prove most effective.

Clan culture, characterized by a high level of internal trust and informal communication, paradoxically creates a favorable environment for targeted phishing that exploits corporate connections. Employees accustomed to mutual assistance and information sharing within the team are more likely to click a link sent in the name of a "colleague from a neighboring department," even if such a request is formally unauthorized [5].

Adhocratic culture (from the English adhocracy, derived from the Latin ad hoc – "for this specific purpose") presupposes the absence of rigid bureaucratization, the temporary nature of working structures, and high tolerance for risk. In the context of information security, this cultural model paradoxically increases vulnerability to phishing, as attackers exploit employees' orientation toward finding "new efficient solutions." Innovation and experimentation are encouraged, generating a risk of interacting with unconventional digital services and tools, which can be exploited by attackers to introduce malware disguised as a useful new application [6].

Thus, the same employee, placed in different cultural contexts, will demonstrate different degrees of vulnerability. Consequently, an effective training and monitoring system must take into account not only the individual characteristics of the employee but also the cultural specifics of their department and the organization as a whole.

Communicative Patterns and their Role in the Legitimation of Phishing Content

This group of factors is associated with the specifics of information exchange organization within a company. Communication channels, their accessibility to external senders, the frequency and nature of information messages shape what employees perceive as a "horizon of expectation" – an idea of which correspondence is normal, legitimate, and does not require additional verification.

A critically important parameter is the intensity of external communications. In departments whose daily activities involve regular interaction with contractors, clients, or government bodies (procurement, sales, legal department), a gradual normalization of contacts with unknown senders

occurs. Employees in such units are highly likely to open attachments and click on links in emails coming from external addresses, since this is a routine part of their work. Attackers, aware of this feature, deliberately disguise phishing messages as commercial offers, reconciliation statements, or requests from regulatory authorities [7].

Equally significant is the level of digitalization of business processes. The higher the proportion of routine operations transferred to the digital environment and automated, the more employees' ability to critically evaluate information messages atrophies [8]. The habit that the system "will check everything itself" and "will filter out dangerous content itself" creates a cognitive automaticity that renders a person defenseless against attacks that successfully bypass technical filters (for example, using compromised legitimate senders or domain spoofing) [9].

The conducted analysis allows us to draw the following fundamental conclusions. First, susceptibility to phishing is not randomly individual but socially structural in nature and can be predicted based on an analysis of the employee's professional role, the type of corporate culture in the department, and the specifics of their communicative tasks. Second, effective information security training cannot be uniform; it must take into account the listed factors and simulate phishing scenarios that are relevant to the actual work context of a specific user. Third, activity monitoring should be aimed not only at recording instances of clicking on malicious links but also at identifying deep-seated sociocultural patterns (for example, excessive trust in internal corporate requests), which can only be corrected at the level of organizational policies, not individual training.

These conclusions form the basis of the user profiling model and the software system architecture developed within this study, which ensures the generation of context-dependent educational phishing scenarios and personalized learning trajectories.

Technical Architecture of the System

Taking into account the factors of susceptibility to phishing and communicative patterns in the corporate environment, the architecture of a software tool implementing the classic three-tier "client – server – database" model was developed, which ensures the logical separation of presentation, application logic, and data storage layers. The client-side component, developed using HTML, CSS, and JavaScript, allows dynamic interaction with the user via AJAX requests to the server API, which in turn allows updating page content without a full reload. The server-side component is built on the Django framework using the Django REST Framework to organize a REST API, through which the client-side sends HTTP requests of methods GET, POST, PUT, and DELETE, and the server returns responses in JSON format (Figure 1).

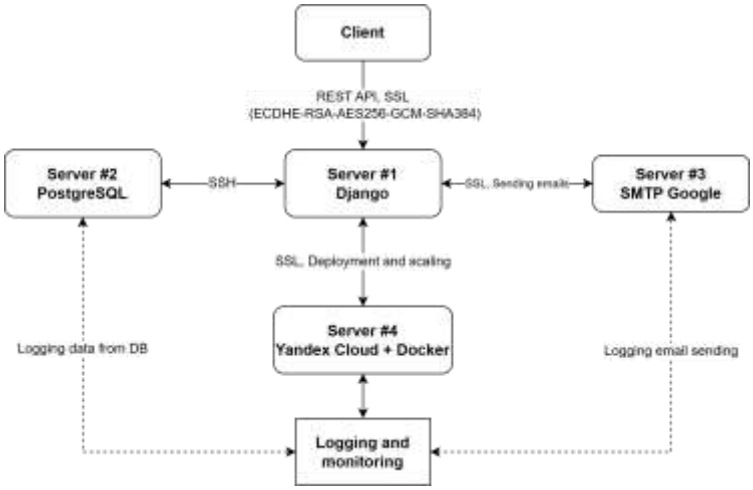

Figure 1: Application functioning scheme

User authentication and authorization are implemented using the django-allauth library with generation of JWT tokens, ensuring secure access to protected resources.

Data management is carried out through the PostgreSQL database management system, with interaction implemented via Django ORM. This approach not only abstracts the developer from

writing low-level SQL queries but also ensures automatic input escaping, which is an effective measure for preventing SQL injection attacks. Logging and monitoring of user activity, including system login, test completion, and interaction with phishing emails, are performed using the django-activity-stream library, followed by data storage in the database and generation of analytical reports.

The phishing attack simulation module deserves special attention. The system administrator creates a phishing email scenario through the interface, after which the server-side component, using standard Python libraries for working with email, performs asynchronous distribution via the Google SMTP server. Asynchronous processing is carried out using Celery, which prevents blocking of the application's main execution thread. All connections to the external SMTP server are secured with SSL/TLS protocols. User reactions to received messages – opening an email, clicking a link, entering data on a fake page – are recorded by the logging module and subsequently used to assess employee awareness levels and adjust individual learning trajectories.

Application security is ensured at multiple levels. In addition to the already mentioned protection against SQL injection via ORM, the system implements protection against cross-site scripting through automatic escaping of data output in Django templates, as well as protection against cross-site request forgery through verification of unique CSRF tokens in each form. All data transmission channels between client and server are secured with the HTTPS protocol. Application containerization is performed using Docker, and deployment and scaling are carried out in the Yandex Cloud environment, which ensures fault tolerance and elasticity of computing resources [10].

Thus, the proposed architecture represents a holistic, modular, and secure solution that integrates user profiling, personalized training, threat simulation, and behavioral monitoring functions into a single framework, thereby enabling a closed-loop management of the human factor in the corporate information security environment.

Integration of Sociological and Technical Components

The system implements a closed loop of "profiling → testing → training → profile correction". Sociological analysis allows identifying not only individual but also group vulnerabilities at the department level, making it possible to address training not only to specific employees but also to department heads for work process correction (Figure 2).

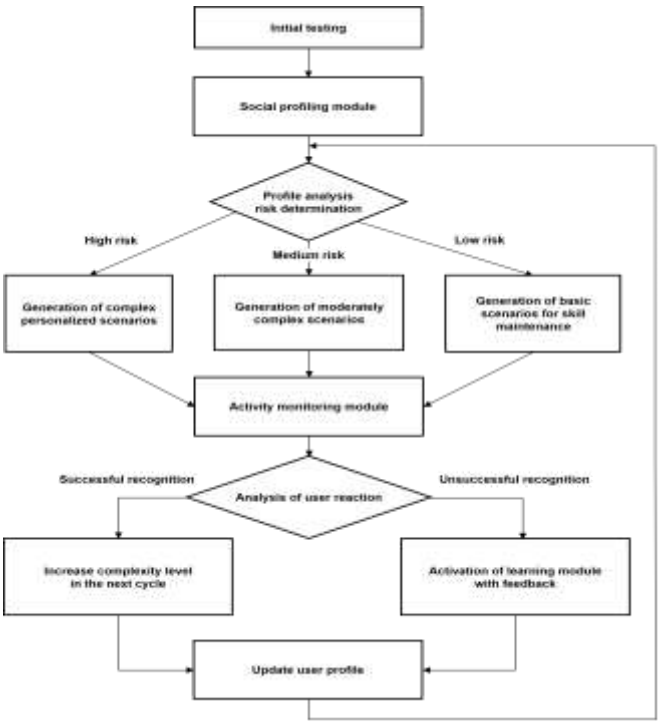

Figure 2: Module interaction scheme

The implementation of user activity monitoring systems to improve information security inevitably creates a contradiction between two competing values: the protection of corporate assets and employees' right to privacy in the digital environment [11]. The software tool being developed, which involves the collection and analysis of behavioral data when interacting with phishing messages, belongs to the class of dual-use technologies, where the line between preventive security and total surveillance is extremely thin. In this regard, the ethical legitimacy of the system becomes not an optional addition but a necessary condition for its practical implementation, since a lack of trust on the part of employees can negate the learning effect and provoke hidden resistance.

The key principle of the proposed approach is "transparency and informed consent." Employees must be informed in advance and in an accessible manner about the existence of the monitoring system, its purposes, the list of metrics collected, and the methods of their processing. Covert observation that is not disclosed in corporate policies or employment contracts is considered unacceptable. The organization's information security policy must contain a separate section regulating the use of phishing simulation tools and behavioral analytics, while employees retain the right to receive clarifications and feedback. It is important to emphasize that educational phishing attacks are not intended for punishment or reprimand; their sole task is to diagnose vulnerabilities and develop sustainable safe behavior skills.

The second foundational principle is the minimization of collected data and its depersonalization. The system architecture is designed so that the object of monitoring is exclusively behavioral metrics: the fact of opening an email, reaction time, clicking a link, entering data on a training phishing page. The content of employees' personal communications, messenger correspondence, and browsing history of websites not related to training scenarios are not subject to collection, storage, or analysis. For generating reports and evaluating training effectiveness, predominantly aggregated information at the level of groups, roles, or departments is used, which allows identifying systemic problems without stigmatizing individual employees. Identification of a specific user is permitted only in cases of persistently repeated risky behavior requiring an individualized learning trajectory, or upon suspicion of malicious actions; however, even in these situations, access to data is strictly limited to authorized security personnel.

Finally, a necessary element of an ethically sound system is regular auditing. Monitoring policies, data processing procedures, and decision-making algorithms must be periodically reviewed for compliance with both changing legislation and the organization's internal ethical codes [12]. It is advisable to involve independent data protection experts in the audit and to form collegial bodies with participation of employee representatives. Only when all three specified conditions – transparency, minimization, and accountability – are met can an activity monitoring system become not an instrument of total control, but a means of fostering a mature information security culture, perceived by employees not as a threat but as a benefit.

The process of registering a new user in the software tool is initiated by the administrator, who sets the employee's login and email address. The system automatically generates a one-time ten-digit password using the `get_random_string` function, and then sends it to the specified email address via an SMTP server, ensuring reliable and secure delivery. The user logs in using the login and temporary password, after which the system, through the `change_password` form, prompts them to change it to a permanent one. The form requests the current password, a new password, and its confirmation; upon successful data validation, the record in the database is updated, and the `update_session_auth_hash` function preserves the user's active session, preventing forced logout. In case of incorrect data entry, the system generates corresponding error messages, informing the user of the need to retry or contact the administrator. A fragment of the functions implementing this is shown in Figure 3.

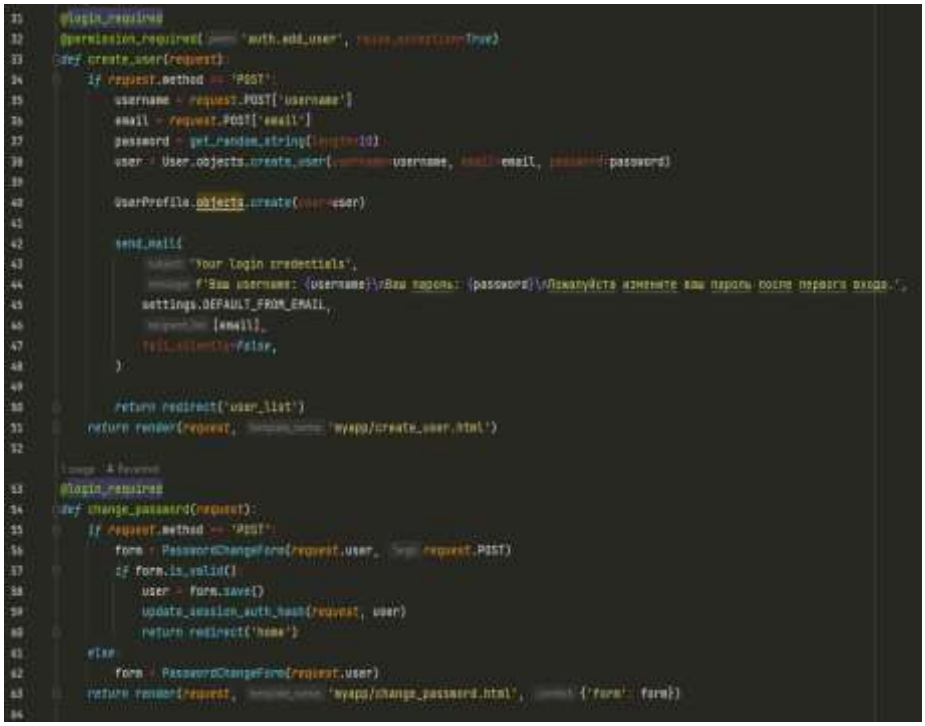

Figure 3: Fragment of user management functions

The creation and editing of training courses is carried out by the administrator, which allows specifying the course name, its detailed description, and attaching additional materials, including graphic images and text documents. When saving an existing course, the form automatically switches to editing mode, updating the corresponding records in the database. Each course can contain an arbitrary number of internal pages, which are managed, allowing the structuring of educational content and building a logical sequence for its mastery. Course deletion is performed with mandatory confirmation of the action by the administrator; the system ensures cascading deletion of all associated pages, uploaded files, and test results, which guarantees database integrity and eliminates the creation of "orphan" records. All operations with courses are available exclusively to users with administrator rights, data transmission is protected by the HTTPS protocol, and each request is verified with CSRF tokens to prevent cross-site request forgery. A fragment of the course management functions is shown in Figure 4.

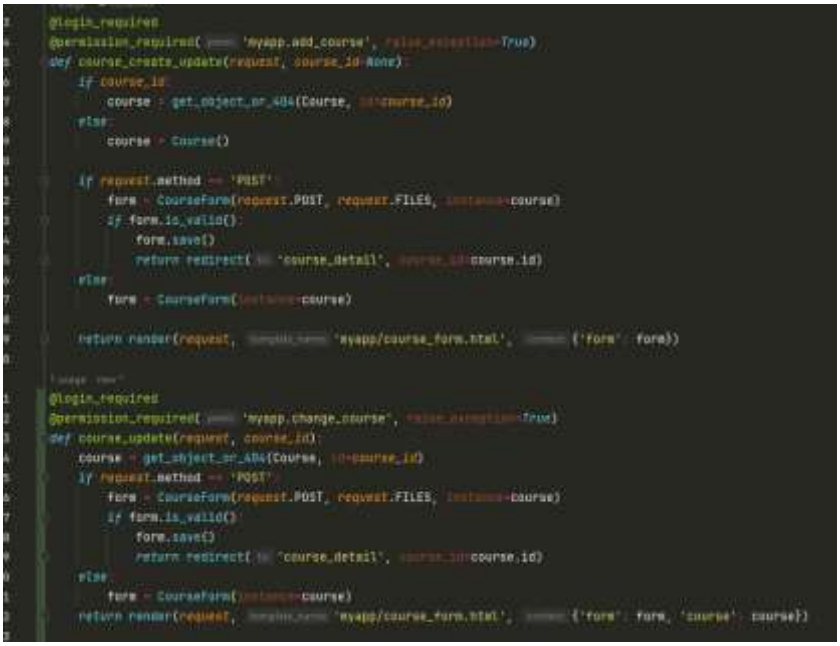

Figure 4: Fragment of course management functions

The creation of test tasks is implemented through the `test_create_update` form, by means of which the administrator specifies the name and description of the test. The test structure includes questions that support various formats: text input, single-choice, or multiple-choice. Editing of tests is also performed via specialized forms with automatic updating of records in the database. A fragment of these functions is shown in Figure 5.

```
@login_required
@permission_required('myapp.add_test', raise_exception=True)
def test_create_update(request, test_id=None):
    if test_id:
        test = get_object_or_404(Test, id=test_id)
    else:
        test = Test()

    if request.method == 'POST':
        form = TestForm(request.POST, instance=test)
        if form.is_valid():
            form.save()
            return redirect('test_detail', test_id=test.id)
    else:
        form = TestForm(instance=test)

    return render(request, 'myapp/test_form.html', {'form': form})

@login_required
@permission_required('myapp.delete_test', raise_exception=True)
def test_delete(request, pk):
    test = get_object_or_404(Test, pk=pk)
    if request.method == 'POST':
        test.delete()
        return redirect('test_list')
    return render(request, 'myapp/test_confirm_delete.html', {'test': test})
```

Figure 5: Fragment of test management functions

The key functional module of the system is the phishing attack simulation tool, accessible via the `send_phishing_email` form. The administrator composes a message, specifies the recipient (a specific employee or a group of users), the subject, the text, and optionally attaches a file. A hidden tracking link to monitor clicks and a tracking pixel to record the fact of opening are automatically embedded into the email body. When the user interacts with the email, the system logs the event: clicking the link is recorded by the track_phishing_email function, opening the email by the track email open view class, and downloading an attachment by the download_phishing_attachment function. Administrators can send phishing emails to users or groups of users. Emails may contain links and attachments, and the system tracks user actions: link clicks, email opens, and attachment downloads. An example of sending a phishing email is shown in Figure 6.

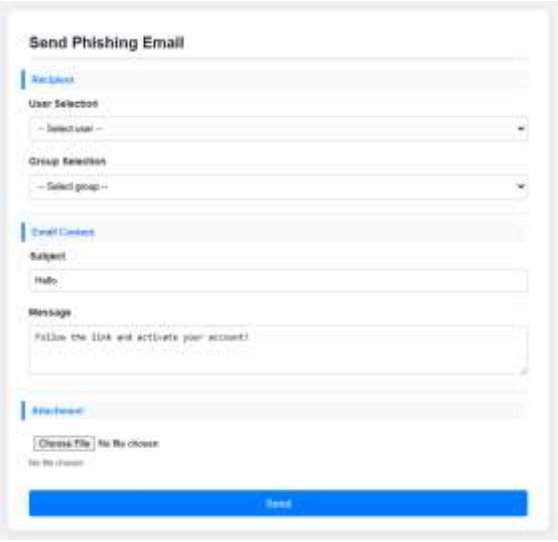

Figure 6: Phishing message sending window

To create an email, the administrator enters the subject, text, and optionally adds an attachment. After successful sending, they are redirected to the report page.

Each event is stored in the database with the user's name and login, the type of action performed, and an exact timestamp. Message distribution is implemented via the Google SMTP server with SSL/TLS encryption, ensuring the confidentiality and integrity of the transmitted information. All collected data is passed to the activity monitoring module for subsequent analysis and visualization. A fragment of the functions for working with phishing messages is shown in Figure 7.

```
def track_phishing_email(request, email_id, user_id):
    phishing_email = get_object_or_404(PhishingEmail, id=email_id)
    user = get_object_or_404(User, id=user_id)
    action.send(user, verb='перешел по фишинговой ссылке', target=phishing_email)
    return redirect('home')

class TrackEmailOpenView(View):
    def get(self, request, email_id, user_id):
        email = get_object_or_404(PhishingEmail, id=email_id)
        follow(request.user, email, send_action='открыл фишинговое сообщение', timestamp=timezone.now())
        return HttpResponse(status=204)

def track_email_open(request, email_id, user_id):
    phishing_email = get_object_or_404(PhishingEmail, id=email_id)
    user = get_object_or_404(User, id=user_id)
    action.send(user, verb='открыл фишинговое сообщение', target=phishing_email)
    return HttpResponse(status=204)
```

Figure 7: Fragment of functions for working with phishing messages

The data on user actions accumulated during the system's operation is aggregated and visualized in the form of analytical reports. The `activity_report` function generates a chronologically ordered event feed, including test completions, opening of phishing emails, link clicks, and attachment downloads, with details for each user. The `test_results_report` function provides testing result statistics, including average scores for each test, grade distribution, and the number of completed attempts. The `user_progress` and `user_progress_report` functions are intended for assessing individual employee progress, displaying the number of courses completed, tests taken, time spent, and the dynamics of result changes.

When a user interacts with an email (clicks a link, opens an email, or downloads an attachment), the system records these actions, storing the data for further analysis. An example of the user interaction window with phishing messages is shown in Figure 8.

User Interaction with Phishing Emails

User	Action	Target / Email Subject	Date
Mikhail Mikhailov (test2)	clicked on phishing link	Please confirm your account - test2	January 13, 2025 19:23
Mikhail Mikhailov (test2)	clicked on phishing link	Please confirm your account - test2	January 13, 2025 19:23
(admin)	sent phishing email	test2	January 13, 2025 19:20
(admin)	sent phishing email	test	January 13, 2025 19:20
(test)	clicked on phishing link	fyv - test	January 13, 2025 02:09
(admin)	sent phishing email	test	January 13, 2025 02:09
(admin)	sent phishing email	test	January 13, 2025 01:45

Figure 8: User interaction window with phishing emails

All report forms are built on the basis of data accumulated by the monitoring module and are available exclusively to system administrators.

Thus, this section has examined in detail the implementation of the key functional modules of the software tool, including authentication and account management mechanisms, educational content administration, test task generation, phishing attack simulation with behavioral tracking, as well as data collection and visualization of analytical data. The structure of component interaction within the system is described, along with corresponding fragments of program code and the libraries used.

RESULTS

This study has confirmed the initial hypothesis that effective counteraction to phishing threats in a corporate environment is impossible within a purely technical approach that ignores the social nature of the human factor. The developed software architecture, integrating sociological analysis of organizational roles, behavioral monitoring, and adaptive learning algorithms, represents a transition from a reactive model of "error correction" to proactive risk profile management. The key result of this work is not so much the software implementation itself, but the proposed sociotechnical method, within which phishing simulations become not a control tool, but a means of diagnosing and developing sustainable safe behavior skills. It has been proven that personalization of training scenarios based on the socio-professional affiliation of the employee (position, department, communication patterns) allows not only increasing the relevance of training but also minimizing the "habituation" effect to repetitive test mailings.

The practical significance of the obtained results is determined by the possibility of their direct implementation in a corporate environment. The expected reduction in the success rate of real phishing attacks by 40–60%, combined with a threefold increase in the speed of response to suspicious messages, creates a measurable economic effect expressed in the prevention of data leaks and financial losses. At the same time, the system does not require a radical restructuring of existing business processes: built on open technologies and standardized protocols, it integrates as an add-on over the organization's already functioning IT infrastructure. It is important to emphasize that the proposed solution is aimed at small and medium-sized businesses, where human and financial resources for in-person training are limited. For such companies, automation of training and competency assessment processes becomes the only accessible way to systematically address the human factor.

CONCLUSION

Further research within this stated direction should be developed along three main trajectories. First, in-depth development of social profiling methods is required, including integration with organizational network analysis systems to identify informal leaders and hidden information dissemination channels that could be exploited by attackers. Second, the implementation of machine learning algorithms for dynamic classification of behavioral patterns and predictive identification of employees entering the risk group, even before they commit erroneous actions, appears promising. Third, longitudinal studies tracking the long-term impact of regular personalized simulations on organizational culture and employee attitudes toward cybersecurity issues are necessary. The combination of these directions will ultimately allow a transition from fragmented training interventions to a holistic human capital management ecosystem in the field of information security, where each employee is viewed not as a potential threat, but as a conscious subject of protective processes.

REFERENCES

1. Data Breach Investigation Report: Most breaches are related to non-malicious human factor (2024) https://newsletter.radensa.ru/archives/6363
2. Ostanin, O. V., Ostanina, E. A.. Training of organization personnel on information security issues. Business. Education. Law (2022). № 2(59). P. 204–209. https://doi.org/10.25683/VOLBI.2022.59.258

3. Demenenko I.A., Romanov P.G. Transformation of corporate culture in modern companies: from theory to implementation // Economics and Management: Problems, Solutions (2025). № 10. T. 11. P.12–18; https://doi.org/10.36871/ek.up.p.r.2025.10.11.002.
4. Kalhoro, S., Rehman, M., Ponnusamy, V., & Shaikh, F. B. Extracting key factors of cyber hygiene behaviour among software engineers: A systematic literature review. IEEE Access (2021). № 9, P. 99339–99363. https://doi.org/10.1109/ACCESS.2021.3094560
5. Alomair, M., Issa, T., Nau, S. Z., & Salih, B. A. The key factors that influence employees' awareness of social engineering: A systematic literature review (2025). Heliyon. № 11(16), e44012. https://doi.org/10.1016/j.heliyon.2025.e44012
6. Yu, J., et al. The shadow of fraud: The emerging danger of AI-powered social engineering and its possible cure (2024). arXiv preprint arXiv:2407.15912. https://arxiv.org/abs/2407.15912
7. Bhusal, C. S. Systematic review on social engineering: Hacking by manipulating humans (2021). Journal of Information Security. №12(2), P. 104–114. https://doi.org/10.4236/jis.2021.122006
8. Obukhov A. D. Automation of information distribution in adaptive electronic document management systems using machine learning, Advanced Engineering Research (2020). V. 20, № 4. P. 430–436. ISSN 2687-1653 https://doi.org/10.23947/2687-1653-2020-20-4-430-436
9. Aldawood, H., Skinner, G. Reviewing cyber security social engineering training and awareness programs — Pitfalls and ongoing issues (2019). Future Internet. №11(3), P. 73. https://doi.org/10.3390/fi11030073
10. Varenitsa, V. V., Markov, A. S., Tsirlov, V. L., et al. How to avoid mistakes in secure software development (2025). Kvant-media. p. 344.
11. Nadeem, M., Zahra, S. W., Abbasi, M. N., Arshad, A., Riaz, S., & Ahmed, W. Phishing attack, its detections and prevention techniques (2023). International Journal of Wireless Security and Networks. №1(2), P. 13–25.
12. Cazares, M., Fuertes, W., Andrade, R., Ortiz-Garcés, I., & Rubio, M. S. Protective factors for developing cognitive skills against cyberattacks (2023). Electronics. № 12(19), P. 4007. https://doi.org/10.3390/electronics12194007
13. Alqahtani, S. Strengthening cybersecurity: The influence of student behavior, perceived factors, and mitigating strategies on phishing attack perception (2025). In International Conference on Cybersecurity and Intelligent Systems. Springer. https://doi.org/10.1007/978-981-96-1483-7_27
14. Koniagaki, A., & Chrysanthou, A. Understanding the role of demographic and psychological factors in users' susceptibility to phishing emails: A review (2025). Applied Sciences. № 15(4), p. 2236. https://doi.org/10.3390/app15042236