Human Factors in Cybersecurity, Vol. 208, 2026, 86–95
https://doi.org/10.54941/ahfe1007415

Simulating the Threat: A Phishing Campaign to Enhance Cyber Resilience in a Large Organization

Leandros Maglaras[1], Kitty Kioskli[1], Antonis Adamakos[2], Stavros Kyriakoudeas[3], Demetris Antoniou[3], and Nestoras Chouliaras[4]

[1]trustilio B.V., Vijzelstraat 68, 1017 HL Amsterdam, The Netherlands
[2]FuzzFree, Athens, Greece
[3]Ianus Technologies, Spyrou Kyprianou 85, Larnaca 6051, Cyprus
[4]Directorate of Primary Education of Viotia, Filonos 35-39, Livadia, Greece

ABSTRACT

The human element remains the most critical, yet often least addressed, vulnerability in organizational cybersecurity. For any company, effective security awareness must evolve beyond static training to include realistic, experiential learning. This report details the planning, execution, and outcomes of a controlled, simulated social engineering phishing campaign conducted within such an organization. The primary objective was to use Social Engineering as a Cybersecurity Awareness Tool to transform passive policy knowledge into active, reflexive cyber-resilience among employees. By providing direct, practical experience with a leading open-access tool like Gophish, followed by training lectures, these campaigns aim to transform phishing exercises from a compliance checkpoint into an integrated, continuous practice.

Keywords: Phishing campaigns, Human factor, Cybersecurity awareness, Social engineering

INTRODUCTION

Phishing is one of the most important and widespread attacks in cybersecurity, with direct and indirect impacts on electronic systems, personal data, and corporate infrastructure. Beyond the purely technical dimension, phishing is the result of deception and the exploitation of human errors and psychological vulnerabilities, which makes it particularly persistent and resistant to technological changes (Birthriya et al., 2025).

Phishing isn't a recent phenomenon; its origins date back to the mid-1990s, when computer network connections became widespread and the internet emerged as a major medium for communication and transactions. The first recorded mass phishing attacks targeted users of the America Online (AOL) platform (Priya et al., 2024, March). Attackers created fake messages, impersonating reliable services or AOL representatives, and asked users to confirm their account details or other sensitive data. Although primitive by today's standards, this initial form of phishing established the psychological patterns that would be used for decades: the pretense of authority, the creation of a sense of urgency or risk, and the appeal to trust.

Received October 25, 2025; Revised April 4, 2026; Accepted April 23, 2026; Available online July 20, 2026

As technology progressed and the economy became increasingly reliant on electronic systems and online transactions, phishing evolved rapidly. In the early 2000s, sophisticated automation tools appeared, enabling less technically skilled attackers to mass-create and distribute phishing emails. Tactics also became more advanced: instead of general mass mailings, targeted attacks began to emerge, utilizing publicly available information to create more convincing messages. The 2000s and early 2010s were characterized by advanced forms of phishing combined with malware, notably the emergence of banking Trojans like Zeus, which could intercept reliable, intermediate sessions while users conducted online banking. More recently, the landscape transformed further with the rise of specialized cybercrime groups and state actors, leading to highly sophisticated spear phishing campaigns against specific individuals or organizations, often requiring prior reconnaissance and person-specific research (Abou El Houda, Z., 2024). Furthermore, attack channels broadened beyond email to include phishing via SMS (smishing), phone calls (vishing), social media, and highly specialized variants like Business Email Compromise (BEC), directly targeting corporate financial cycles. The integration of Artificial Intelligence technologies, especially Large Language Models (LLMs) (Ferrag et al., 2025) and deepfake voice and video synthesis, enabled the creation of hundreds of thousands of hyper-personalized phishing messages and highly realistic synthetic media that are nearly indistinguishable from authentic content (Afane et al., 2024 December).

The human element remains the most critical, yet often least addressed, vulnerability in organizational cybersecurity. For any company, effective security management must include an awareness program that should evolve beyond static training to include realistic, experiential learning (Maglaras et al., 2022). The integration of this awareness program into the security mechanisms of the company through repetitive phishing campaigns and focused training sessions can help organizations raise their security levels (Almomani et al., 2021) and avoid major cyberattacks. As stated in previous works (Brunken et al., 2023), large organizations often have heterogeneous technical infrastructures and training requirements. Selecting the right product or service for an organization requires time and effort from multiple stakeholders, thereby inducing a high final cost. In this paper, we present a recent phishing campaign design and execution on a large company, following a structured methodology and analysis.

Human Factors Considerations in Phishing Susceptibility

Phishing attacks frequently succeed by exploiting inherent human limitations in attention, perception, and decision-making rather than purely technical vulnerabilities. For instance, a recent eye-tracking study showed that when inspecting phishing emails many users' visual focus drifts away from critical cues such as sender identity or actual hyperlink URLs and instead lingers on superficial elements like masked links or generic body text, which significantly increases phishing susceptibility (Zhuo et al., 2023). Related work further emphasizes that email presentation including how

links are rendered, whether a button or a text link, and the device used (mobile vs desktop) affects click behavior, with masked links and mobile devices substantially increasing the probability of users clicking malicious links (Musuva et al., 2019). These findings illustrate that even users with baseline security awareness can be misled under normal working conditions: when cues are subtle and cognitive workload is high, the brain relies on fast heuristics, making phishing a fundamentally "human-factors" problem rather than strictly a technical one.

Beyond perceptual factors, more recent empirical evidence shows that broader psychological and contextual variables, such as personality traits, organizational context, and email workload, also shape phishing vulnerability. A 2025 study demonstrated correlations between certain personality traits (e.g., higher extraversion, agreeableness, and neuroticism) and greater susceptibility to phishing, suggesting that individual differences influence how users process potentially malicious emails (López-Aguilar et al., 2025). Another recent organizational-level study found that demographic and job-related factors, not just knowledge level, significantly affect both phishing susceptibility and incident-reporting behavior among employees (Desolda et al., 2022). These results underscore that phishing defenses should not rely solely on training or technical filters but also account for human variability, organizational culture, and contextual stressors. As a human-centric conclusion, designing effective phishing prevention requires a holistic approach: combine interface design (clear link presentation, warning cues), adaptive organizational policies, and awareness of human behavioral diversity to reduce reliance on fast, error-prone heuristics.

Methodology

The work presented in this paper details the steps followed for conducting a successful phishing campaign. The process followed a structured methodology, commencing with a rigorous planning and scoping phase, essential for a corporate environment. We also conducted a thorough market analysis of available Phishing Tools to select a solution offering high customizability and detailed logging. This was used as an input to the tooling and infrastructure setup, ensuring the campaign infrastructure could mimic real-world threat actors while remaining completely isolated from production systems. Critically, extensive effort was dedicated to legal and ethical considerations (Greco et al., 2024, October). This involved securing formal approval from executive leadership, establishing a clear opt-out mechanism, and ensuring all collected data was anonymized and used strictly for educational and aggregate reporting purposes.

To select the correct platform to use, we had to choose between open source and proprietary platforms. Since the main goal was to create a campaign that could be easily replicated on several occasions and was mainly an educational tool, we decided to focus only on open source tools that could be both powerful and efficient (Blancaflor et al., 2021). The initial market analysis led to these 4 candidates:

- **Gophish:** This is a popular open-source phishing framework designed for businesses and penetration testers. It provides a web interface to easily set up and execute phishing campaigns, track results (email opens, link clicks, credential submissions), and analyze effectiveness.
- **Social-Engineer Toolkit (SET):** A Python-driven open-source tool widely used for social engineering penetration testing. It can be used to simulate various attacks, including credential harvesting.
- **King Phisher:** Another powerful tool for simulating phishing attacks, often used to educate users about the dangers of phishing.
- **Evilginx:** A powerful man-in-the-middle (MITM) attack framework that can bypass two-factor authentication (2FA) by intercepting session tokens. It can be integrated with Gophish for campaign management.

Analyzing these options and having in mind that, except for efficiency, we wanted the tool to be user-friendly, highly customizable, and able to provide real-time results and analytics, we decided to use Gophish, using also the comparative analysis by previous research (Sahay et al., 2024). Gophish is highly regarded as a strong open-source phishing framework primarily because it is designed for ethical use by security professionals and penetration testers to conduct realistic phishing simulations and security awareness training. Its key strength lies in its user-friendliness, featuring a web interface that simplifies the creation and management of sophisticated campaigns (See Figure 1). Users can easily customize email templates and landing pages to mimic real-world threats, utilize dynamic personalization for a more believable lure, and launch campaigns across various operating systems. Crucially, Gophish provides real-time results and detailed analytics, tracking metrics like email opens, link clicks, and credential submissions, which gives organizations the actionable data they need to measure employee vulnerability and effectively enhance their security posture over time.

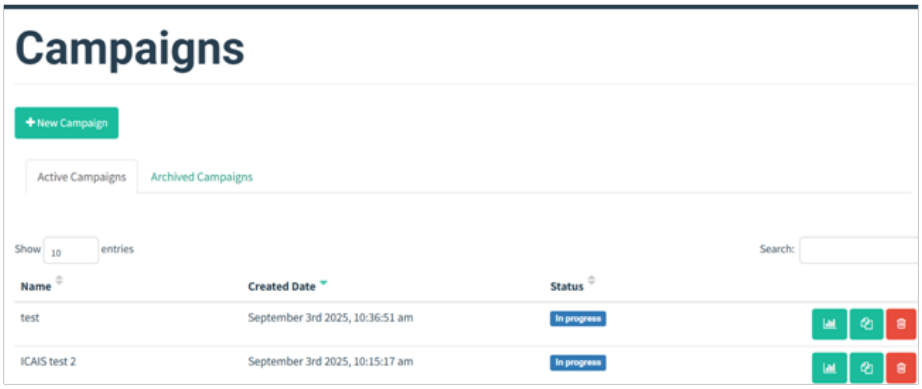

Figure 1: Gophish campaign design internal system.

The campaign setup involved a sophisticated attack vector development and execution, which focused on a single, highly effective lure. For this phishing campaign, we designed a sophisticated email targeting the common institutional practice of securing external funding. The simulated email utilized specific

European Commission branding, contact details, and a plausible subject line ("Tender application call number EU.6/43/2025") to create high urgency and legitimacy. Sent from a spoofed address, the email falsely notified the recipient that their tender status was "pending," requiring immediate confirmation (see Figure 2). The campaign was executed in phased waves, targeting a statistically significant sample group across departments involved in grant writing and external collaboration. Success metrics were focused on two key actions: the click rate (clicking the embedded link) and the credential submission rate (entering credentials on the malicious landing page).

Dear tender applicant,

There has been an update regarding your call number **EU.6/43/2025**. The call status has changed to pending. To continue the process, the pending status requires your confirmation in the eProcurement Portal

Use the portal https://tenders.ec-europa.eu/apply to examine your tender application.

Kind regards,

[redacted]
Head of Unit

European Commission
DG Grow
Unit C.2 – European Citizen Action Service
MADO 26/003
B-1049 Brussels/Belgium
[redacted]

European Union

This message was sent automatically by the European Commission eProcurement Portal. Please do not reply to this email.

Figure 2: Phishing email from the 1st campaign.

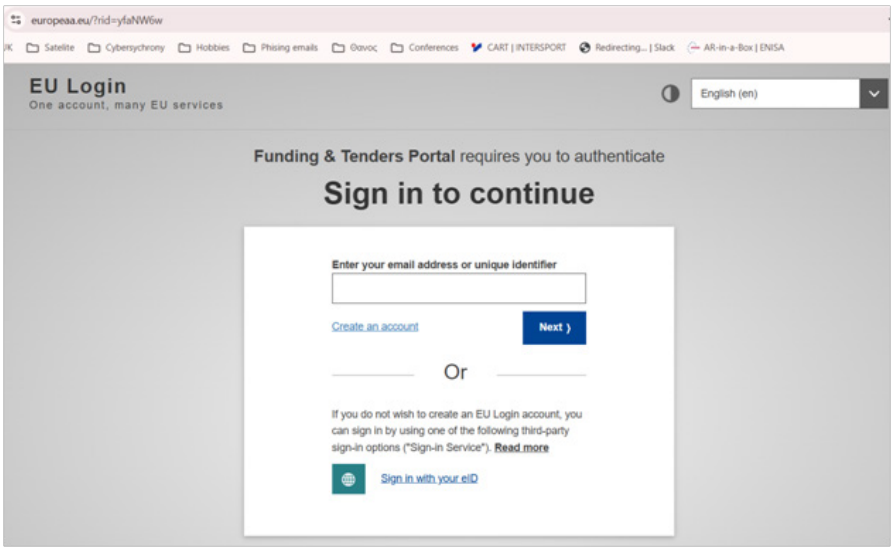

Figure 3: The loading webpage where the victim is asked to add their information.

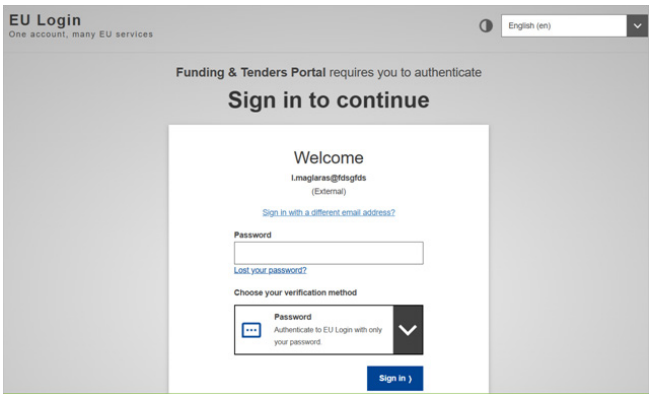

Figure 4: The victim is asked to add username and password but this information is not captured in Gophish.

Analysis of Findings

Based on the information collected from Gophish we analyzed the click rate with respect to different roles inside the company and the evolution of the response as the attack was continuing to take place for over 4 hours. In Table 1, we see the roles of the employees who were included in the campaign inside the company, along with the number of those who clicked and submitted data. Figure 5 shows the dashboard of Gophish, while Figure 6 shows detailed information about each user's behavior against the attack. We can see from Figure 6 that a specific user tried several times to enter data (username, password) without noticing that the website was fake.

Table 1: Roles of employees in the company.

Role	Number of Employees	Clicked	Entered Data
Researcher	9	4	3
Lawyer	1	0	0
Developer/ S. Developer	6	1	1
Deputy	1	0	0
Head of IT	1	0	0
Content creator	1	0	0
Chief Business Operator	1	0	0
CEO, Deputy, Technical Director	3	2	0
Secretary	1	0	0
other	6	0	0

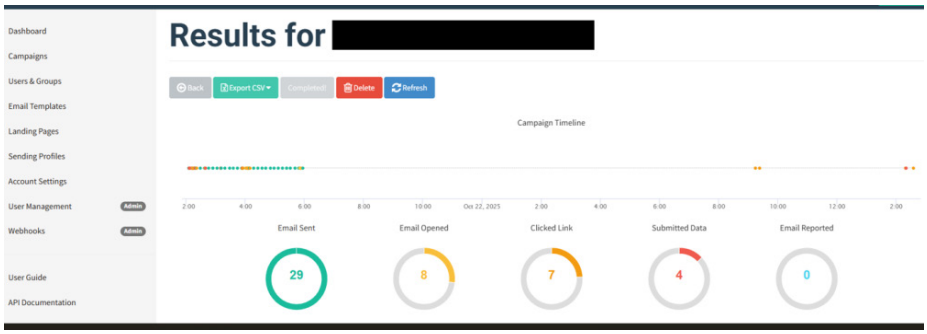

Figure 5: Gophish statistics about the emails sent during the campaign (sent, opened, clicked, submitted data, reported).

Researchers were the most at-risk group, in which 4 out of 9 clicked the link, or 44.4%, and 3 followed through with credential disclosure, or 33.3%. This higher risk is attributable to the fact that this campaign specifically manipulated the targets' work environment: staff members accustomed to frequent applications for grants and tenders are psychologically primed to consider correspondence from the European Commission as legitimate and urgent.

Technical personnel were relatively more resilient. Of the developers and senior developers, only 1 out of 6 clicked on the phishing link and further submitted data-16.7%. The Head of IT did not interact with the malicious content at all. The tendency here is that technical exposure to cybersecurity threats, added to less direct involvement in external funding processes, gave them some natural resistance to this particular attack vector.

The leadership responses were a mixed bag. Of the executive cadre-that is, the CEO, Deputy, and Technical Director-2 of 3 clicked on the phishing link, 66.7%, yet none submitted credentials. This difference would indicate that even as initial engagement took place, perhaps due to the relevance of tender communications to strategic operations, further evaluation prevented full compromise. However, the high click rate among top executives does point to the fact that rank does not guarantee any sort of immunity against sophisticated social engineering attacks.

A specifically instructive observation emerged from the detailed behavioral analytics captured in Figure 6: one individual persistently attempted to submit credentials without recognizing indicators of the site's fraudulent nature. This pattern illustrates how initial cognitive commitment to a perceived legitimate interaction can override subsequent critical evaluation a well-documented phenomenon in social engineering literature that reinforces the necessity of pre-engagement verification training.

These role-stratified findings carry significant implications for remediation strategy. Rather than uniform awareness training, organizations should consider differentiated educational interventions calibrated to occupational risk profiles. Personnel whose responsibilities involve regular engagement with external funding bodies, regulatory communications, or high-value transactions warrant prioritized and context-specific training modules addressing the precise psychological triggers exploited in targeted spear-phishing campaigns.

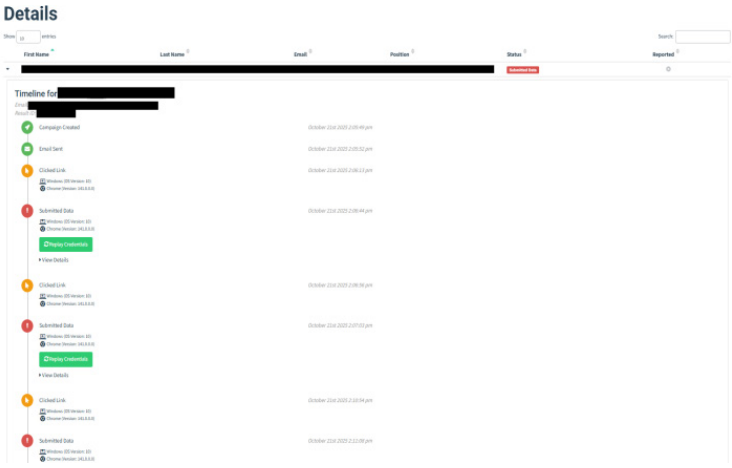

Figure 6: Detailed reporting about each employee regarding the phishing campaign.

CONCLUSION

The Further Analysis, Reporting, and Education phase is the next step to follow. Our initial results provide a quantitative baseline of the organization's vulnerability, identifying the specific psychological triggers exploited by the tender lure and quantifying the overall organizational risk profile. This raw data will be translated into a comprehensive report for leadership, detailing aggregate vulnerability scores, time-to-first-click metrics, and observed behavioral patterns.

The campaign must be followed by mandatory, immediate, and targeted remediation. All employees who participate in the test will receive a non-punitive training module focusing on identifying highly spoofed government/tender communications, and will be presented with an organization-wide presentation that deconstructs the campaign and reinforces best practices for verifying external communications.

Finally, these campaigns can be used for establishing a framework for Continuous Improvement and Iteration. The baseline metrics gathered serve as a benchmark for future campaigns, adapting the complexity of the lures based on the organization's current performance. This iterative approach allows the organization to measure the sustained impact of the training, adapt to emerging threat trends like highly targeted spear-phishing, and foster a proactive, security-conscious culture.

This paper demonstrates that ethical, simulated social engineering, even with a single, highly tailored vector, is an invaluable, high-fidelity instrument for hardening a research-centric organization from the inside out. The goal of the campaign was to analyze the available phishing tools in the market, choose the open source tool that could effectively be used in our campaigns (Gophish), perform the planning, set up the infrastructure, deal with Legal and Ethical Considerations, and finally run the 1st campaign (Attack Vector Development and Execution).

ACKNOWLEDGMENT

The authors would like to acknowledge the financial support provided for the following projects: The 'Advanced Cybersecurity Awareness Ecosystem for SMEs' (NERO) project, which has received funding from the European Union's DEP programme under grant agreement No. 101127411; and the 'Harmonizing People, Processes, and Technology for Robust Cybersecurity' (CyberSynchrony) project, which has received funding from the European Union's Digital Europe Programme (DEP) under grant agreement No.101158555. The views expressed in this paper represent only the views of the authors and not those of the European Commission or the partners in the above-mentioned projects. Finally, the authors declare that there are no conflicts of interest, including any financial or personal relationships, that could be perceived as potential conflicts.

REFERENCES

Abou El Houda, Z. (2024). Cyber threat actors review: examining the tactics and motivations of adversaries in the cyber landscape. In *Cyber Security for Next-Generation Computing Technologies* (pp. 84–101). CRC Press.

Afane, K., Wei, W., Mao, Y., Farooq, J., & Chen, J. (2024, December). Next-generation phishing: How LLM agents empower cyber attackers. In *2024 IEEE International Conference on Big Data (BigData)* (pp. 2558–2567). IEEE.

Almomani, I., Ahmed, M., & Maglaras, L. (2021). Cybersecurity Maturity Assessment Framework for Higher Education Institutions in Saudi Arabia. *PeerJ Computer Science*, *7*, e703.

Birthriya, S. K., Ahlawat, P., & Jain, A. K. (2025). Detection and prevention of spear phishing attacks: A comprehensive survey. *Computers & Security*, 104317.

Blancaflor, E. B., Alfonso, A. B., Banganay, K. N. U., Cruz, G. A. B. D., Fernandez, K. E., & Santos, S. A. M. (2021). Let's go phishing: A phishing awareness campaign using smishing, email phishing, and social media phishing tools. In *Proceedings of the International Conference on Industrial Engineering and Operations Management, no. Sanchez* (pp. 260–269).

Brunken, L., Buckmann, A., Hielscher, J., & Sasse, M. A. (2023). "To Do This Properly, You Need More {Resources"}: The Hidden Costs of Introducing Simulated Phishing Campaigns. In *32nd USENIX Security Symposium (USENIX Security 23)* (pp. 4105–4122).

Desolda, G., Ferro, L. S., Marrella, A., Catarci, T., & Costabile, M. F. (2022). *Human Factors in Phishing Attacks: A Systematic Literature Review*. Musuva, P., Getao, K. W., & Chepken, C. K. (2019). *A New Approach to Modelling the Effects of Cognitive Processing and Threat Detection on Phishing Susceptibility*.

Ferrag, M. A., Tihanyi, N., Hamouda, D., Maglaras, L., & Debbah, M. (2025). From Prompt Injections to Protocol Exploits: Threats in LLM-Powered AI Agents Workflows. *arXiv preprint arXiv:2506.23260*.

Greco, M., Chang, R., & Galdames, P. (2024, October). Educational Phishing: An Awareness Campaign to Learn How to Detect Phishing. In *2024 43rd International Conference of the Chilean Computer Science Society (SCCC)* (pp. 1–5). IEEE.

López-Aguilar, P., García-Villalba, L. J., Al-Nashashibi, A., & Al-Dosari, F. (2025). Phishing Vulnerability and Personality Traits: Insights from a Systematic Investigation. Journal of Information Security and Applications. Elsevier.

Maglaras, L. (2022). From mean time to failure to mean time to attack/compromise: incorporating reliability into cybersecurity. *Computers*, *11*(11), 159.

Priya, S., Gutema, D., & Singh, S. (2024, March). A comprehensive survey of recent phishing attacks detection techniques. In *2024 5th International Conference on Innovative Trends in Information Technology (ICITIIT)* (pp. 1–6). IEEE.

Sahay, R., Meng, W., & Li, W. (2024, October). A Comparative Analysis of Phishing Tools: Features and Countermeasures. In *International Conference on Information Security Practice and Experience* (pp. 365–382). Singapore: Springer Nature Singapore.

Zhuo, S., Biddle, R., Betts, L., Arachchilage, N. A. G., Koh, Y. S., Lottridge, D., & Russello, G. (2023, April). What You See is Not What You Get: The Role of Email Presentation in Phishing Susceptibility. In Proceedings of the 18th Symposium on Usable Privacy and Security (SOUPS). USENIX Association.