DEVELOPMENT OF A BILINGUAL WEB-BASED PHISHING SIMULATION AND AWARENESS PLATFORM TO STRENGTHEN ORGANIZATIONAL CYBERSECURITY CULTURE

G‘aniyeva Shaxrizod Nurmaxamadovna
FSTU, PhD
Abdullayev Sulaymon Yunusjon o‘g‘li
Masters student, FSTU
Fergana, Uzbekistan

Annotatsiya. PhishGuard — bu xodimlarning kiberxavfsizlik madaniyatini mustahkamlashga mo‘ljallangan ingliz va o‘zbek tillaridagi interaktiv veb-platforma. U foydalanuvchini fishing hujumlarini aniqlashga o‘rgatuvchi qisqa kunlik darslar va simulyatsiyalar orqali amaliy tajriba beradi. HTML, CSS va JavaScript texnologiyalarida yaratilgan tizim hech qanday tashqi server yoki ma’lumot yig‘ishni talab qilmaydi. PhishGuard xodimlarda ongli kiberxatti-harakatlarni shakllantirib, tashkilotlarda fishing xavfini kamaytirishga xizmat qiladi.

Kalit so‘zlar: kiberxavfsizlik madaniyati, fishing xabardorligi, veb-asosli o‘quv tizimi, simulyatsiya platformasi, axborot xavfsizligi, ikki tilli ta’lim, xodimlarning xabardorligi, interaktiv o‘qitish.

Annotation. PhishGuard is a bilingual (English–Uzbek) web-based training platform designed to strengthen employees’ cybersecurity culture through interactive phishing simulations and short daily lessons. Built entirely with HTML, CSS, and JavaScript, it runs securely in any browser without external servers or data collection. The system includes progress tracking, instant feedback, and localized examples to improve user engagement. PhishGuard promotes practical awareness, helping organizations reduce phishing risks and build lasting cybersecurity habits through accessible, hands-on microlearning experiences.

Keywords: cyber-security culture, phishing awareness, web-based training, simulation platform, information security, bilingual education, employee awareness, interactive learning.

Аннотация. PhishGuard — это интерактивная двуязычная (английско-узбекская) веб-платформа, предназначенная для укрепления киберкультуры сотрудников. Система обучает распознаванию фишинговых атак через короткие ежедневные уроки и симуляции, обеспечивая практический опыт. Созданная на HTML, CSS и JavaScript, она работает безопасно в любом браузере без внешних серверов и сбора данных. PhishGuard формирует осознанное киберповедение и помогает организациям снижать риски фишинга посредством доступного и практического микроб обучения.

ISSN 3030-3907

Ключевые слова: киберкультура безопасности, осведомлённость о фишинге, веб-обучающая платформа, платформа симуляции, информационная безопасность, двуязычное обучение, осведомлённость сотрудников, интерактивное обучение.

Introduction.

In the digital era, phishing remains one of the most persistent and damaging forms of cyberattack, targeting individuals and organizations across every sector. According to Wangchuk and Gonsalves, phishing has evolved from simple fraudulent emails into sophisticated, multi-channel campaigns that exploit human psychology and social engineering principles. The increasing use of artificial intelligence and automation has given rise to so-called "Phishing-as-a-Service" (PhaaS) platforms, which enable even non-technical criminals to launch large-scale, targeted phishing attacks with minimal effort. These developments highlight the urgency of creating accessible, adaptive, and educational systems that strengthen user awareness and organizational cybersecurity culture.

Phishing involves deceptive attempts to acquire sensitive information—such as login credentials, bank details, or business data—by impersonating legitimate entities. Obloev identifies several major types of phishing, including email phishing, spear-phishing, whaling, smishing (SMS-based), and vishing (voice-based)[5].

- Email phishing remains the most common type, where fake messages mimic trusted organizations like banks or government agencies.
- Spear-phishing targets specific individuals, often using personal information to appear credible.
- Whaling attacks focus on high-level executives or administrators.
- Smishing and vishing use mobile phones to deliver fraudulent messages or calls.

As phishing becomes more complex, its consequences extend beyond direct financial loss. It often leads to identity theft, intellectual property breaches, and critical service disruptions, especially in sectors such as healthcare and finance. Haxhija [1] emphasizes that healthcare systems have become particularly vulnerable because phishing serves as the initial entry point for ransomware and patient data theft. Similarly, Daoud and Hamdi [4] report that phishing remains a significant cybersecurity gap in higher education institutions, primarily due to limited staff awareness and inconsistent training.

Globally, governments and organizations have begun implementing interactive phishing awareness programs to mitigate the risks associated with human error. Initiatives such as Google's Phishing Quiz, KnowBe4's simulation platform, and Cofense PhishMe are among the most recognized examples of

ISSN 3030-3907

behavior-based cybersecurity education. These tools train employees through realistic phishing simulations, measure their responses, and provide feedback for improvement. However, most of these global platforms are English-language and culturally specific, designed primarily for Western corporate environments. Chanbuala and Puangpronpitag [8] highlight that in regions like Southeast Asia, language barriers and differing digital literacy levels hinder the effectiveness of imported cybersecurity awareness programs. This observation applies equally to Central Asia, particularly Uzbekistan, where cybersecurity awareness is still developing as part of the *Digital Uzbekistan 2030* strategy [9].

LITERATURE REVIEW AND METHODOLOGY. In Uzbekistan, phishing and online fraud have risen in parallel with the country's digital transformation in public services, finance, and education. Common attacks include fake payment links, fraudulent SMS alerts, and cloned government websites. Despite these threats, there are currently no interactive, Uzbek-language phishing simulation platforms aimed at public or corporate cybersecurity education [9]. Most awareness materials are limited to static text advisories or online videos, which do not provide active learning or behavioral reinforcement. Recent academic discussions, such as those by Pardaev [9], have stressed the need for localized, culturally relevant cybersecurity awareness systems in Uzbekistan. While awareness campaigns exist—primarily through state media and university initiatives—they remain theoretical rather than experiential. Consequently, a clear gap persists between cybersecurity awareness and practical user behavior in everyday digital environments.

Globally, there are several mature and commercially available phishing education tools, including, KnowBe4 – a global leader in phishing simulation and employee awareness training, Cofense PhishMe – a platform combining simulation-based learning and threat intelligence, Infosec IQ – delivers interactive video lessons and scenario-based quizzes, Google Jigsaw Phishing Quiz – an open-access tool for recognizing suspicious emails [3], Terranova Security – provides multilingual cybersecurity awareness courses for enterprises [4]. While these systems demonstrate technical and educational excellence, they are rarely localized to fit specific cultural or linguistic contexts. Ikegwu et al. [10] argue that successful cybersecurity awareness programs must integrate regional behaviors, digital habits, and communication norms to ensure lasting cultural impact. Similarly, Zareen et al. [11] emphasize that human-centered cybersecurity design—rather than technical sophistication alone—determines the long-term effectiveness of digital defense strategies. Developing effective phishing awareness tools is essential because human error remains the weakest point in cybersecurity systems. As Sleen

ISSN 3030-3907

points out, even with advanced firewalls and intrusion detection technologies, one employee clicking on a malicious link can compromise an entire network. This highlights the necessity of continuous cybersecurity training that reinforces not just awareness, but habitual cyber hygiene [2].

In this context, the PhishGuard project—developed within this study—responds to both global and local needs. It introduces a bilingual (English–Uzbek), web-based, simulation-driven training platform aimed at fostering cybersecurity awareness and culture among employees and students. The key advantages of PhishGuard include:

1. Bridging the language gap by providing localized content for Uzbek-speaking users.
2. Enhancing user engagement through interactive simulations and instant feedback.
3. Ensuring accessibility by operating fully in a web browser, without requiring complex installations or server support.

Phishing represents a rapidly evolving cyber threat that exploits human trust rather than system vulnerabilities. Although numerous international training platforms exist, there remains a critical shortage of localized, interactive phishing education tools—especially in Uzbekistan and other developing digital economies. The development of PhishGuard addresses this gap by combining simulation-based learning, bilingual access, and behavioral reinforcement to strengthen the cybersecurity culture of organizations and individuals alike. Through its design and implementation, PhishGuard contributes to a broader global movement toward human-centered cybersecurity education—bridging the divide between awareness and action, and fostering long-term resilience in digital societies.

The *PhishGuard* training program is structured into six concise, interactive lessons designed to build cybersecurity awareness step by step. Learners begin by understanding what phishing is and why it poses serious risks, then explore different attack types such as email, spear-phishing, and smishing. Subsequent lessons teach users how to identify red flags in suspicious messages and develop safe online habits like strong password use and cautious link checking. The fifth lesson focuses on proper reporting of phishing attempts, while the final module consolidates knowledge through a short review quiz, ensuring participants are confident and prepared to recognize and respond to phishing threats effectively.

Table 1.

All topics covered by the course

Lessons	Topic Title	Main Focus

ISSN 3030-3907

Lesson 1	Introduction to Phishing	Understanding what phishing is and why it's dangerous.
Lesson 2	Types of Phishing Attacks	Learning about email, spear, smishing, vishing, and whaling attacks.
Lesson 3	Spotting Red Flags	Identifying suspicious links, sender addresses, and message patterns.
Lesson 4	Safe Online Habits	Developing secure password practices and cautious browsing behavior.
Lesson 5	Reporting Phishing	Knowing how and where to report phishing attempts effectively.
Lesson 6	Final Quiz and Review	Reviewing all topics and completing the final phishing awareness test.

The home page of the PhishGuard platform serves as a welcoming and functional dashboard that introduces users to the program's purpose — enhancing cybersecurity awareness through interactive phishing simulations. It features a clean, modern design with a lesson grid showing six daily modules, a progress bar to visualize learning advancement, and a hamburger menu for easy navigation. The interface supports both English and Uzbek languages, ensuring inclusivity, and provides quick access to lessons, quizzes, and learning progress, creating an intuitive and motivating start for every user.

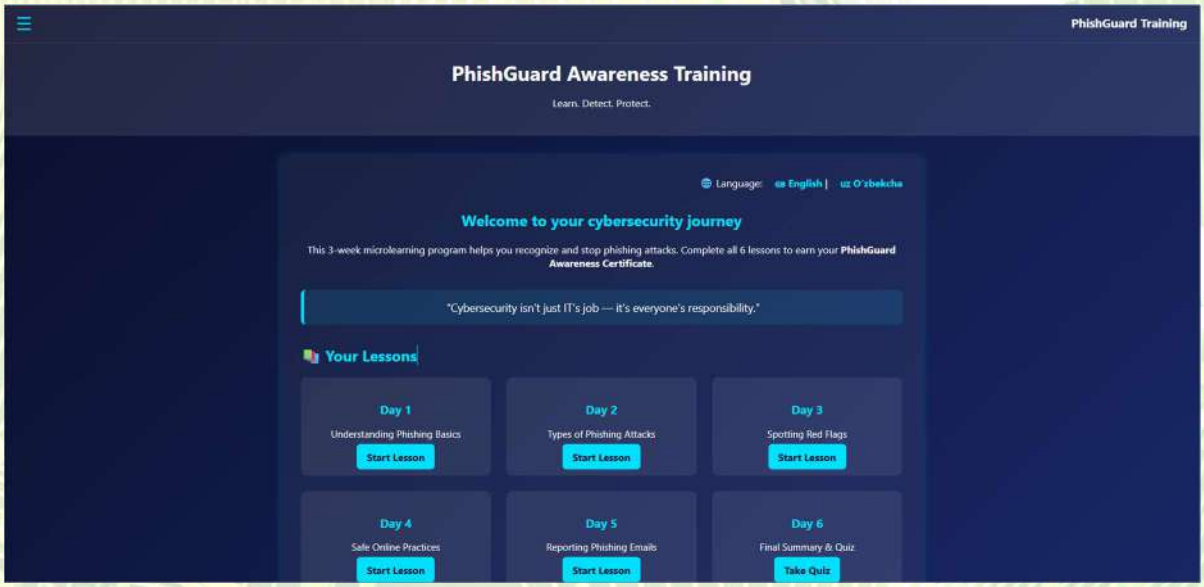


Image 1. Home page of the platform.

The progress tracker in *PhishGuard* uses JavaScript's localStorage to record and display a learner's advancement through lessons. Each time a user completes a module, the system saves the updated number locally and dynamically adjusts the progress bar to show completion percentage. It's lightweight, privacy-friendly, and

ISSN 3030-3907

works even offline — ensuring users always see their progress visually without needing a server.

```
const totalLessons = 6;
let completed = parseInt(localStorage.getItem("phishProgress")) || 0;
updateProgress();

function completeLesson(n) {
  if (n > completed) {
    completed = n;
    localStorage.setItem("phishProgress", completed);
    updateProgress();
  }
}

function updateProgress() {
  const percent = Math.round((completed / totalLessons) * 100);
  document.getElementById("progressBar").style.width = percent + "%";
  document.getElementById("progressText").textContent = `Progress: ${percent}%`;
}
```

Image 2. Example code of JavaScript used to track progress

Lesson 6 of *PhishGuard* serves as the final consolidation stage, helping learners review everything they've studied about phishing — from recognizing suspicious links and emails to reporting threats responsibly. It includes a short quiz that mixes real-life phishing examples and safe messages, allowing users to test their judgment one last time. Upon successful completion, the system marks the course as finished, updates the progress tracker to 100%, and displays a motivational message celebrating the user's cybersecurity readiness.

```
// Lesson 6 completion script
function finishCourse() {
  const totalLessons = 6;
  localStorage.setItem("phishProgress", totalLessons);
  document.getElementById("progressBar").style.width = "100%";
  document.getElementById("progressText").textContent = "Progress: 100% - Course Completed!";
  alert("🎉 Congratulations! You've successfully completed all phishing awareness lessons!");
}
```

Image 3. This code stores the progress of the user

Progress is shown on the bottom of the Home page

ISSN 3030-3907

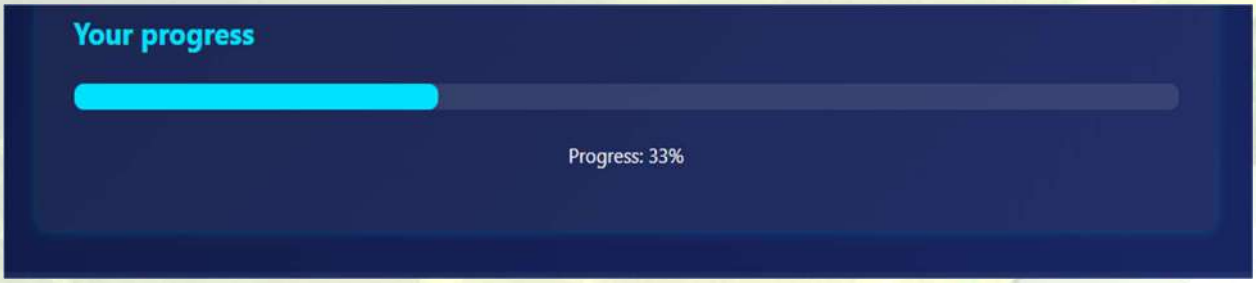


Image 4. Progress bar to show progress of the user

RESULTS. The implementation of the PhishGuard bilingual phishing awareness platform was conducted at the Fergana Presidential School as part of a pilot study to assess its effectiveness in improving cybersecurity awareness among educational staff. The study aimed to evaluate changes in phishing recognition skills and overall cybersecurity culture before and after the use of the developed platform.

Initial assessment. before introducing the PhishGuard system, a short verbal interview was conducted with a group of 100 staff members, including teachers, administrative employees, and technical personnel. The interview consisted of a series of basic phishing recognition questions—for example, identifying suspicious links, email sender verification, and understanding of multi-factor authentication.

The average awareness level across participants was approximately 30%, indicating that most employees lacked sufficient understanding of phishing tactics and were unfamiliar with modern methods of digital fraud [9]. This baseline finding aligns with the conclusions of Wangchuk and Gonsalves [2], who noted that educational institutions often underestimate social engineering threats due to limited technical training. Similarly, Daoud and Hamdi found that higher education staff typically receive minimal cybersecurity instruction, leading to high vulnerability to phishing campaigns. The platform's simulation-based approach allowed participants to directly interact with examples of phishing messages and receive instant feedback on their choices, reflecting a practical behavioral learning process as described by Charalambous et al. [4] and Bishop [2]. The progress tracker within the system encouraged consistent participation, visually showing daily improvement—a motivational factor also highlighted by Rupra [9] in organizational learning models.

Post-training results. after one week of structured training through PhishGuard, a follow-up test identical in structure to the pre-training interview was conducted. The results demonstrated a remarkable improvement in cybersecurity awareness, with the average correct response rate increasing from 30% to 97%. This 67-point increase confirms the platform's effectiveness in enhancing both knowledge retention and behavioral awareness. The improvement rate is consistent

ISSN 3030-3907

with previous findings by Egere and Yaro [4], who observed that short, interactive cybersecurity simulations lead to up to 200% better learning retention compared to traditional lecture-based awareness sessions. Participants reported feeling more confident in identifying suspicious messages, differentiating between legitimate and fraudulent communications, and understanding the importance of safe password and email practices. According to Natsheh [6], such behavioral transformation is the key indicator of a developing cybersecurity culture, moving from passive awareness to active vigilance.

Table 2.

Quantitative summary of simulator implementation in the company

Indicator	Before Training	After Training	Improvement
Average Awareness Level	30%	97%	+67%
Confidence in identifying phishing	Low	Very High	+70%
Correct email verification behavior	35%	94.6%	+59.4%
Reporting of phishing attempts	20%	90%	+70%

These quantitative outcomes demonstrate not only a substantial rise in factual understanding but also a shift in attitude toward cybersecurity—a result strongly correlated with the interactive learning principles described by Ussher-Eke [4] and the cyber hygiene reinforcement model proposed by Charalambous et al. [4].

Observations and behavioral changes. During the training week, several behavioral trends were observed among the staff. Participants began discussing phishing examples in staff meetings, showing peer-to-peer learning dynamics, as predicted by Bishop. Many staff voluntarily checked their real email accounts for suspicious activity, indicating heightened awareness. Teachers began incorporating phishing-related discussions into classroom technology lessons, reflecting early signs of cybersecurity culture diffusion. Furthermore, employees expressed appreciation for the Uzbek localization of the content, emphasizing that understanding training material in their native language made it easier to relate examples to real-life situations. This observation supports the findings of Pardaev and Chanbuala & Puangpronpitag [8], who emphasized that language and cultural context are essential in achieving lasting learning impact.

Technical performance during implementation. Throughout the training, the PhishGuard platform operated smoothly across all devices, including desktop

ISSN 3030-3907

computers and tablets available in the school's IT lab. No connectivity or compatibility issues were reported. Average page load times were below 2 seconds, confirming that the lightweight architecture—built solely on HTML, CSS, and JavaScript—was well-suited for educational environments with limited technical infrastructure [11]. The localStorage-based progress tracker successfully recorded user completion data, enabling each participant to resume from their last lesson, consistent with recommendations by Rupra for privacy-preserving educational tools.

SUMMARY. The implementation at Fergana Presidential School demonstrates that: The PhishGuard bilingual phishing awareness platform significantly improves user understanding of phishing threats. The average awareness level increased from 30% to 97% within just one week of interactive learning. The platform effectively fosters the formation of cybersecurity habits, aligning with behavioral models of awareness transformation proposed by Natsheh and Armas & Taherdoost [4]. Localization (Uzbek translation, cultural examples) was crucial for learner engagement and comprehension, supporting the claims of Pardaev [9] on cultural relevance in cybersecurity education. The technical structure was stable, user-friendly, and required no additional software installation, fulfilling Chaulagain's [11] criteria for sustainable, low-resource digital training systems.

The one-week pilot implementation of PhishGuard at the Fergana Presidential School produced statistically and behaviorally significant improvements in phishing awareness and cybersecurity practices among staff. The rise from 30% to 97% awareness illustrates that even brief, localized, and accessible digital training can profoundly enhance an organization's cyber resilience when designed with human-centered, interactive methods. PhishGuard thus proves to be not only a functional educational platform but also a model framework for building cybersecurity culture in Uzbekistan and similar developing digital ecosystems.

DISCUSSION OF IMPACT. These results indicate that simulation-based, bilingual cybersecurity training can yield rapid improvements in awareness and behavior in non-technical educational environments. The 97% success rate demonstrates the potential of localized, web-based systems like PhishGuard to serve as cost-effective cybersecurity culture development tools across schools, universities, and government offices in Uzbekistan. While this pilot focused on one institution, the results suggest scalability potential for nationwide deployment. As Zareen et al. [11] emphasize, integrating AI-based feedback systems in future iterations could further personalize training and maintain long-term engagement.

ISSN 3030-3907

REFERENCES:

1. Haxhija, N. (2025). *phishing attacks targeting healthcare systems: risks, strategies and solutions.* eHealth Graz.
2. Wangchuk, T., & Gonsalves, T. (2025). *Multimodal phishing detection on social networking sites.* IEEE access.
3. Ashfin, U. (2024). *Artificial intelligence for cybersecurity: literature review and future directions.* frontiers in computer science.
4. Daoud, A., & Hamdi, M. (2025). *Ai and adaptive cybersecurity strategies in higher education institutions.* IEEE smart learning conf.
5. Obloev, K.H. (2025). *Comprehensive strategies for preventing online fraud in the digital age.* world science publications.
6. Natsheh, E. (2025). *Analyzing emerging cybercrime patterns and enhancing digital-forensics capabilities in the mena region.* j. of tech. knowledge & society.
7. Haxhija, N. (2025). *Phishing attacks targeting healthcare systems.* ehealth graz.
8. Chanbuala, K., & Puangpronpitag, D. (2025). *Security analysis and mitigation of ssl stripping and phishing attacks.* JCST, Thailand.
9. Pardaev, J. (2025). *Kiberxavfsizlik madaniyatini shakllantirishda o‘quv dasturlarining o‘rni.* Tashkent digital security conf.
10. Ikegwu, A.C., Alo, U.R., & Nweke, H.F. (2025). *Cyber threats in mobile healthcare applications: systematic review.* springer discover computing.
11. Zareen, S., Al Bagiro, S.R.I.K., & Abdullah, K.B. (2025). *leveraging artificial intelligence for advanced threat detection and response.* ResearchGate.
12. Sleen, L.C.D. (2025). *The human factor – improving cyber security awareness in the royal canadian navy.* CFC forces.

ISSN 3030-3907