Gamified Phishing Awareness Training Platform for Corporate Employees using Unity

Pallavi V Patil
Department of Computer Science and Engineering
Dayananda Sagar University
Bengaluru, India pallavivpatil3280@gmail.com

Sanika K S
Department of Computer Science and Engineering
Dayananda Sagar University
Bengaluru, India kssanika11@gmail.com

Namala Navya Sree
Department of Computer Science and Engineering
Dayananda Sagar University
Bengaluru, India nnavyareddys@gmail.com

Dr Prabhakar M
Department of Computer Science and Engineering
Dayananda Sagar University
Bengaluru, India
prabhakar.m-cse@dsu.edu.in

How to Cite this Article:

Patil, P. V., S, S. K. & Sree, N. N. (2026). Gamified Phishing Awareness Training Platform for Corporate Employees using Unity. International Journal of Creative and Open Research in Engineering and Management, 02(04). https://doi.org/10.55041/ijcope.v2i4.958

https://doi.org/10.55041/ijcope.v2i4.958

***Abstract*—**Phishing problems are still a significant contributor to data breach, and human error is the cause of approximately 68 percent of data breaches globally. Companies invest in security training programs, but it is quite often that they are not effective since the employees might not pay attention, remember the information and fully comprehend how the actual phishing attacks can be used. In order to fill this gap, the present paper proposes PhishGuard, a training system in the form of a game that is able to enhance phishing awareness and response.

PhishGuard is built in Unity and provides a realistic and interactive learning experience. Unlike most of the available training tools on cybersecurity, it uses a simulation of a real office environment, which enables users to associate training with their work environment. The system also produces phishing emails that describe six major attack categories, including emails claiming to be an executive or IT personnel. The paper singles out the main shortcomings of existing training technologies: they are not realistic, have a low ratio between difficulty levels and response feedback, and are not well integrated into companies learn systems, and include a limited selection of phishing techniques. PhishGuard is solving these problems with five main features. To begin with, it provides a virtual office experience that is realistic. Second, it contains an adaptable phishing email creator. Third, it gives adjustment

of difficulty depending on the performance of the user. Fourth, it offers instant feedback, which enables the users to learn. Lastly, it monitors user activity and creates performance reports to companies.

In general, PhishGuard will help to make cybersecurity training more interactive, realistic, and quantifiable. Integrating gamification with a real-life simulation enables employees to be more aware of phishing attacks and prevent them, which enhances the security of organizations.

Index Terms—Phishing awareness; gamification; Unity; serious games; security awareness training; corporate cybersecurity; adaptive learning; social engineering; xAPI; BEC fraud.

I. INTRODUCTION

Phishing is a problem. It is when someone sends an email or message to trick people into giving away important information, like passwords or money. This is the common way that organizations get attacked and it can be very expensive.

The 2024 Verizon Data Breach Investigations Report said that people making mistakes contributed to 68% of all data breaches. IBMs report said that the average cost of a data breach is around USD 4.45 million and phishing is usually the starting point of these attacks.

The energy sector is a target for cyberattacks. In the United Kingdom it was targeted 24% of the time in 2021. To fight this organizations have spent a lot of money on Security Awareness Training programs. These programs are often just videos or online courses that people have to watch once a year. Research shows that these programs do not work well because people do not remember what they learned and they do not feel like they are really learning anything.

A study found that 82% of data breaches happened because someone made a mistake. This means that the training programs are not working. Gamification is a way of teaching people about cybersecurity. It uses game- elements, such as points and rewards to make learning more fun and interesting. Studies have shown that gamification can help people learn more and remember what they learned.

There are some tools that use gamification to teach people about phishing and cybersecurity. There are still some big gaps. No one has made a tool that uses an office simulation to teach people about phishing. No one has made a tool that can adjust the difficulty level based on the persons job. How well they are doing.

This paper is about a tool called Phish Guard. Phish Guard is a game- platform that teaches people about phishing in a realistic office simulation. It adjusts the difficulty level based on the person's job. How well they are doing. The paper talks about the following things:

- A review of existing tools. What is missing
- A plan for how to build Phish Guard
- A framework for designing phishing scenarios
- A way to test how well Phish Guard works
- A comparison of Phish Guard with tools

Phish Guard is a Unity-based platform that puts people in a realistic 3D office simulation. They have to navigate through phishing scenarios and get feedback on how they're doing. The difficulty level adjusts based on their job. How well they are doing. This paper is, about how Phish Guard can help people learn about phishing and how it can be used in organizations.

II. RELATED WORK

A. Conventional SAT and Its Limitations

The conventional SAT interventions, i.e. instructor-based workshops, video-based compliance modules, and email-based knowledge tests have been largely criticized as yielding inadequate behavioural change. Workers often feel that compulsory training is intrusive to the work process, lowering actual participation [3], [4]. The systematic literature review by Khando et al. on the subject of information security awareness among both the private and the public organizations gave a conclusion that passive formats do not tackle the affective aspect of security behaviour change [4]. Ahmed et al. found that traditional methods could no longer be effective in instilling information security culture because they do not have the motivation and practical components that can facilitate the acquisition of skills in the face of realistic threat scenarios [7]. This evaluation is supported by the fact that the human component of more than two-thirds of breaches persists despite extensive investment in SAT [1].

B. Gamification in Cybersecurity Education

Gamification uses game features, such as points, badges, leader boards, levels, and storytelling, in non-game settings to boost motivation, engagement, and performance [5]. In cybersecurity education, gamified methods have shown clear effectiveness. Ahmed et al. created a Capture the Flag (CTF) style web platform using Root the Box to teach smart grid users about security awareness at three difficulty levels: beginner, intermediate, and advanced [7]. Their study found that participant scores improved by 40%, 35%, and 29% respectively across these levels. This supports the idea that increasing difficulty helps learning. The study also highlighted the benefits of hint-based training. Participants who used more hints during training tended to recover better in the evaluation stage.

Pantaliano et al. designed ForenSEEK, a serious game for digital forensics awareness that uses Unity Engine and Augmented Reality (AR) to target young adults in the Philippines [9]. Their pre-test and post-test study with 150 participants showed knowledge improvement from 54% to 77% (paired t-test: t=8.35, p=6.18E-14). The game received a high satisfaction rating of 6.29 out of 7 on the Game User Experience Satisfaction Scale (GUESS), with 82.67% of participants finding the feedback mechanism effective. ForenSEEK proves that Unity-based serious games can be used in cybersecurity education and validates the GUESS evaluation tool for this area.

Kostic´ and Saveljic created "Lockedout," a Unity-based game for password strength training that uses both traditional rule-based checking and a third-order Markov model for harder levels [10]. Their work showed how flexible Unity's C scripting is for real-time interactive cybersecurity training, how effectively Scriptable Object-based content management can be used, and how possible it is to integrate probabilistic models into game-based security education. These examples are directly relevant to Phish Guard's proposed implementation.

C. Anti-Phishing Training Tools and Serious Games

There are a number of anti-phishing training solutions that have been created and tested. Phish Guru is an embedded training platform that provides instructional communication when users attach simulated phishing links in the course of their regular email interactions [11]. A randomized controlled study of 515 participants (including control, single-training, and multiple-training conditions) showed that Phish Guru users remembered the knowledge after 28 days and that reinforcement training did not decrease the willingness to click valid links, which is essential to deploying Phish Guru to an enterprise. What.Hack is a role-playing game (RPG) based on the document-checking serious game Papers, Please (Pope, 2013), which educates on phishing emails identification in context [12]. It offers players a progressive rule set, decision making objectives, and instant feedback to tell them about the implications of their decisions. A comparative study proved What.Hack more efficient (over 30 percent better than the previous non-contextual anti-phishing games), crediting the difference to encoding specificity: simulated environment learning that is analogous to the context in which the application will be used. BenAoumeur suggested OfficeGuard, an anti-phishing game written in Unity, which places a player in a three-dimensional office to either label emails as valid or phishing [13]. The most similar existing precedent of PhishGuard is the OfficeGuard which has a significant contribution to the concept. But OfficeGuard was specifically aimed at high school and college students, not at corporate workers; it is based on a fixed number of ten emails with no adaptive difficulty; it is not personalized in roles; it gives feedback in binary correct/incorrect feedback; and it does not publish any evaluation data. These constraints identify the main design space which PhishGuard will deal with. The platform of the SAWIT (Security Awareness Improvement Tool) offers AI-based modular security training via a knowledge-transformation model, which offers collaborative based learning and assessment in an interactive format [3]. Although SAWIT is a useful tool in delivering knowledge in a structured manner it lacks the gamification of the immersive simulation and lacks the fidelity of a 3D environment and contextual scenario.

D. Unity as a Development Platform for Serious Games

The cross-platform game engine of Unity Technologies is one of the most used development platforms in the world, supporting game development in 2D and 3D, AR/VR integration with the AR Foundation and ARCore/ARKit, and deployment on desktop, mobile, and web platforms [15]. Its C# scripting system, Universal Render Pipeline (URP) of high performance rendering, Scene management, Physics engine, and Asset pipeline are very appropriate to the development of serious games. Singh and Kaur presented a detailed, technical description of the core systems of Unity such as scene management, Inspector/Hierarchy architecture, rigid body physics, and asset import workflow [15].

ForenSEEK showed the successful implementation of Unity to the educational game on cybersecurity through the use of AR [9], and Lockedout showed the flexibility of C# scripting on real-time security assessment [10]. All these precedents confirm that Unity is the right platform of PhishGuard.

III. RESEARCH GAPS

Based on the review above, the following five critical gaps in Unity-based and gamified phishing awareness training for corporate employees are identified and documented: G1: Absence of a Corporate-Context Immersive Environment

The closest Unity-based analog, OfficeGuard [13], is created to operate with student populations and a simplified 3D office with low environmental fidelity. No publicly available Unitybased platform offers a high-fidelity corporate office simulation, with role-specific contextual features (finance workstation, IT helpdesk console, HR inbox, executive desk) although simulating specific contexts context-faithful simulation environments have been shown to yield better knowledge transfer to real-world environments [12]. Corporate workers are best trained when their attack scenarios reflect their reallife daily email environment, communication conventions, and the organizational structure.

G2: Lack of Adaptive, Role-Based Scenario Personalization

Current gamified SAT solutions either have fixed library of scenarios or offer rough, large scale difficulty levels. No Unity-based platform is published and dynamically adjusts the difficulty and typology of phishing scenarios, depending on real-time employee performance metrics and position in the organization. This is important due to role-specific targeting of attackers: finance employees are most prone to CEO fraud and wire-transfer scams; IT employees are most likely to be targeted by credential harvesting and helpdesk impersonation; HR employees are most likely to receive fake payroll-change and recruiting emails. Personalization has become a major distinguishing factor of good training [16] but is not available in immersive game-based instruments. G3: Insufficient Real-Time Indicator-Level Feedback

What.Hack [12] and OfficeGuard [13] offer a basic correct/incorrect feedback and do not specify phishing red flags in each case (e.g., there is a mismatched sender domain, the urgency language, the suspicious extension of an attachment, the lookalike URL). ForenSEEK showed that properly developed feedback module can lead to the significant increase of the learning outcomes: 82.67% of the participants found it to be effective [9]. Contextual, indicator-based feedback explaining why an email is a phishing attempt and why it is not is necessary to develop transferable detection capabilities to be used against new real-life attacks, and no current Unity platform can provide such at the necessary level of granularity. G4: No Enterprise LMS Integration and Compliance
Reporting

To be adopted into corporate settings, SAT tools should be able to connect with enterprise Learning Management Systems (LMS) like Moodle, Cornerstone On Demand, or SAP Success Factors, through SCORM or xAPI (Tin Can API) standards. The currently available Unity serious games are standalone research prototypes that do not have a published LMS integration pathway. This loophole does not allow the organizations to monitor the progress of individual employees over time, produce compulsory compliance reports, correlate training completion with latter phishing vulnerability, and identify high-risk employees that may need additional intervention.

G5: Inadequate Discussion of modern Corporate Phishing Types

The majority of tools based on games are concerned with generic phishing (spoofed log-in pages, suspicious links). Modern corporate phishing incorporates spear phishing, Business Email Compromise (BEC), impersonation of the IT helpdesk, payroll-change fraud, QR-code phishing, and multistage attacks which take place over multiple days. These typologies are common in enterprise setting yet they are lacking in the current game-based training platforms. This dynamic attack taxonomy should be included in a corporate oriented platform to ensure a platform stays operationally relevant [17].

IV. PROPOSED PLATFORM: PHISHGUARD

A. Overview and Design Philosophy

Phish Guard essentially comprises of a unity based application that can be implemented as a standalone software for both WINDOWS and macOS. The employee is placed in a realistic 3D environment simulation of work space in which they have personally recognized themselves well in, as if they feel at home enough to make a difference. There are three guiding principles which shape the entire structure of the system. The first principle is called Context Fidelity whereby each and every scenario has to truly represent the nature of the corporate email system in the real world including the attack patterns, the organizational hierarchy and other intricate details[12]. Secondly, there's the Adaptive

Challenge – the difficulty that can be modified depending on the level of success an individual employee has had, ensuring everyone with experience stays challenged while not going beyond the edge [16]. The third factor, Actionable Feedback, involves feedback being provided for each choice that is made by either players or employees – and it's not just about right or wrong answers, but giving a reason that will allow them to recognize phishing threats on their own the next time around. It clearly addresses one of the platform's key objectives and speaks to what research says about the impact of embedded messages [11].

The design of the platform is based on the gamification framework put forward by Landers, where game mechanics perform dual roles. First, it moderates and secondly, it mediates. Moderation occurs when the game mechanics moderate employees to remain highly motivated to participate with the training module. On the other hand, mediation occurs when the mechanics mediate for the deliberate and repetitive practice required to attain mastery of the skills [9]. It is quite easy to align the platform design with the Self-Determination Theory, which suggests that individuals flourish when their psychological needs are satisfied. Competence is fostered by providing employees with increasingly difficult challenges. Employees develop autonomy by determining the best response to the emails they receive. Employees develop a sense of relatedness due to departmental leader boards and badges awarded to the employees' teams.

B. System Architecture

The Phish Guard architecture is made up of five highly integrated components, as seen in Fig. 1. The architecture is organized in layers: the presentation layer from Module 1 contains the immersive simulation component; the logic layer from Modules 2 and 3 provides scenario selection and adaptation capabilities; the learning layer from Module 4 handles instructional feedback; and the data layer from Module 5 controls the game state, analysis, and reporting to the enterprise level. Data travels in a unidirectional path through each layer from the actions of the employee, and then back to the analysis module that updates the competence model of the adaptive engine.

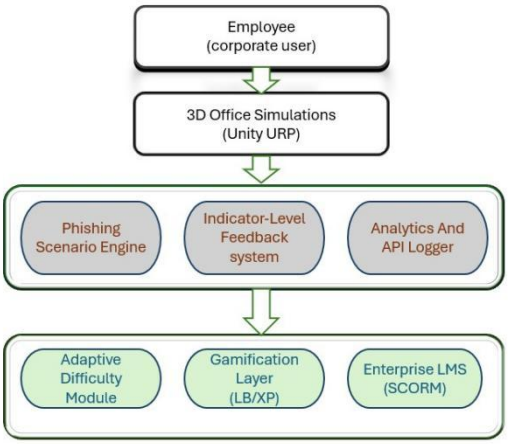

Fig. 1. Proposed Phish Guard System Architecture. Arrows denote primary data/control flow.

C. Module 1 – 3D Corporate Simulation Environment

The simulation will be created in Unity. The rendering technique used will allow the simulation to run on standard business desktop PCs. The environment consists of an office that includes workstations with a high level of detail.

•Computers' monitors have a pre-installed email client application.

•Notifications and alerts pop up when accessing the shared drive.

•Intranet browser windows and documents are placed on the workstations' desks.

The office is segmented by departments.

•Finance Floor - computers for trading;

•HR Office - documents regarding employees;

•IT Helpdesk - server equipment;

•Executive Suite - furniture.

These departmental environments allow employees to immerse themselves in the simulation. It is possible to easily load different department settings using the Unity Scene system. Thus, it will be feasible to have one application for all roles. NavMesh is used for character locomotion within the environment. The user is able to navigate the office between departments. The user can communicate with his or her colleagues. Colleagues provide hints for phishing scenarios. For instance, the finance colleague may refer to a wire transfer.This will enhance the immersion of a subsequent email regarding business email compromise.Interaction with the environment is realized via the Unity Event System.It uses something called Raycast to detect when you click on the user interface and objects you can interact with.

D. Module 2 – Phishing Scenario Engine

The Scenario Engine has a collection of phishing scenario templates. These templates are organized by the type of attack and how hard they are. All of these templates are made using something called Unity Scriptable Objects. This means that people who create security content do not need to know how to code to make, update and keep track of scenarios. They can do all of this without having to rebuild the engine.

Each template has a lot of information. It includes the name of the person who is sending the email their email address, the subject of the email and the content of the email. The content can even have formatting. There can also be attachments and links in the email. The template even says what kind of phishing attack it is and how likely it is to be real or fake. It also says what the right thing to do is when you get the email.

Phish Guard has a way of organizing these scenarios into six types of attacks. These are the kinds of attacks that businesses need to worry about. The first type is called Generic Phishing. This is when someone tries to get you to go to a website or click on a suspicious link. The second type is called Spear Phishing. This is when someone uses your name and information about you to try to trick you. The third type is called BEC or CEO Fraud. This is when someone pretends to be a boss and asks you to do something that could hurt the company. The fourth type is called IT Helpdesk Impersonation. This is when someone pretends to be from the IT department and asks you to give them your login information. The fifth type is called HR Impersonation. This is when someone pretends to be from the human resources department and asks you to give them information. The sixth type is called QR-Code Phishing. This is when someone sends you an email with a QR code that takes you to a website.

The Scenario Engine can load these templates from a folder on the server. This means that new scenarios can be added without having to rebuild the application. This is important because new phishing attacks are coming out all the time. The Scenario Engine needs to be able to keep up with these attacks.

Phish Guards scenario taxonomy includes all of these types of phishing attacks. The Scenario Engine is very good at managing all of these scenarios. It can help businesses protect themselves from phishing attacks. The Scenario Engine and Phish Guard are important tools, for businesses. They can help keep businesses from phishing attacks.

E. Module 3 – Adaptive Difficulty Module

When the program starts for the time, each employee has to answer five questions. This helps figure out what department they belong to, like Finance or HR and how good they are at security training.

The program keeps track of how good each employee's, at security training. It does this by storing information on the employees, computer and sometimes sending it to a server. This information includes a score from 0 to 100 and how good they're at different types of attacks. It also keeps track of how questions they answered correctly how long it took them to answer and what level of difficulty they are at.

After each question the program calculates a score. It does this by looking at if they got the question right or wrong how fast they. If they used any hints. If they got it right they get points. If they answered fast they get points. If they used hints they lose points.

The program has levels of difficulty. To move to the level employees, need to get a high enough score. If their score gets too low, they might have to go to a easier level. The program tries to give employees a variety of questions so they do not get too good at one type of question. It makes sure that no one type of question is than 40% of the questions they have answered recently.

The program is trying to prevent something called skill tunnelling. This is when someone gets really good at one thing but not good at things. The program wants employees to be good, at all types of security training, not one type [7].

F. Module 4 – Indicator-Level Feedback Subsystem

When you make a decision in a scenario the Feedback Subsystem shows you a panel. This panel is like a summary of what you did. It has four parts.

1) Decision Verdict: this part tells you if your answer was correct or not. It does this with a red banner.
2) Indicator Callout Overlay: if you are looking at a phishing email this part highlights the parts of the email. It does this by putting a box around the text and making the box blink. When you put your mouse over the box it tells you why that part of the email is suspicious. For example, if the email is pretending to be from a company but the address is not quite right it will say something, like “this domain looks like the one but it is not”.
3) Social Engineering Principle Panel: this part explains why the email is trying to trick you. It tells you what kind of trick it is using, like pretending to be someone or trying to make you hurry. It also gives you an example of how this trick has been used in the world.
4) Recommended Action: this part tells you what you should do. If the email is phishing it will tell you how to report it and even lets you practice reporting it with one click.

If you correctly identify an email as legitimate the system will tell you that you did a job. It will also break down why the email is legitimate so you can learn what to look for in the future. This helps you get better at recognizing emails and avoids you reporting too many emails that are actually okay. The Feedback Subsystem is helping to fix a problem that was not being addressed before. It is using a method that has been proven to work[9].

G. Module 5 – Gamification and x API Analytics Layer

The Gamification Layer is what makes the platform motivating. Employees get Experience Points for doing things. They get ten Experience Points for identification. If they do it without using any hints they get five Experience Points. If they are keep getting it, they get extra points. For example, if they get five answers in a row their points are multiplied by one and a half. If they get ten answers in a row their points are multiplied by two.They add up as Experience Points. The department leader boards update continuously and display such results. Employees also earn badges for achievements in their activities. For example, they earn a badge named "Phish Detector" for the first recognition of a phishing attack. They earn the badge "BEC Expert" for recognizing five consecutive attacks. They get the "Zero-Click Hero" badge for completing the training session without making any mistake. The badge "Mentor" is earned by completing the team challenge.The Skills Dashboard shows performance statistics in graphs. The graph depicts employees' skill levels in defending against six kinds of phishing attacks. Employees receive information on their performance during the training process.The application records all events that occur during the training. These events include experience points received,responses (right or wrong answers), whether they apply hints, and time spent in debriefing. All these events are sent to a learning record store through a database via the Tin Can API protocol. The protocol works based on web requests, which can manage network failures. The information is useful for the training managers as they can evaluate the operation of the process and make necessary adjustments. On the other hand, the security managers receive valuable information on the performance of employees needing special attention. They can do this without having to look through everything.

V. EVALUATION METHODOLOGY

Once we implement our intervention PhishGuard, its success can be evaluated through a test involving the use of a control group in a manner similar to ForenSEEK. We will apply this intervention on employees of various departments in the organization such as finance, information technology, and human resources. Our sample size will comprise not less than 150 employees for each group.

We will arbitrarily allocate employees to either the PhishGuard group or the group that will undergo video training. There are several indicators we will use to measure the success of the intervention. These include:

• Employees' capability to identify phishing emails before and after video training.
• Number of employees clicking phishing emails sent to them two weeks after video training.
• Number of employees reporting suspicious emails.

• Employees' memory four weeks after the training session.

We shall conduct comparisons of both pre and post-test findings within the respective group as well as make comparisons of the findings across groups. This is done in order to determine whether the training program has different efficacies against various types of phishing scams. Furthermore, we shall also seek the views of the test participants concerning the efficacy of the program through the completion of a questionnaire following the training process. The questionnaire will address issues such as the ease of use the levels of enjoyment experienced as well as whether there are barriers that might hinder the transferability of the acquired knowledge into daily practice. This is done through a focus group discussion with participants. Some data will be obtained from the logs such as the number of people that complete each of the scenarios, frequency of hints required as well as time spent on each task.

VI. COMPARATIVE ANALYSIS

Table I illustrates the functionality of PhishGuard in relation to six other available tools.

Ten criteria have been considered for evaluating the performance of each tool.

The table utilizes symbols, such as:

•✓ indicates full functionality

•~ indicates partial functionality

•× indicates no functionality

TABLE I

COMPARISON OF PHISHING TRAINING PLATFORMS

Feature / Capability	What.Hack [12]	Office Guard [13]	Forensic [9]	Phish Guru [11]	Root the Box [7]	Phish Guard (Proposed)
Unity 3D Engine	×	✓	✓	×	×	✓
Corporate Office Environment	~	~	×	×	×	✓
Role-Based Phishing Scenarios	×	×	×	~	×	✓
Adaptive Difficulty (Dynamic)	×	×	×	×	~	✓
Indicator-Level Feedback	~	~	✓	~	×	✓
BEC / CEO-Fraud Scenarios	×	×	×	~	×	✓
QR / Smishing Scenarios	×	×	×	×	×	Planned
xAPI / LMS Integration	×	×	×	~	×	✓
Multiplayer / Team Mode	×	×	×	×	✓	Planned
Published Evaluation Data	✓	×	✓	✓	✓	Proposed

From the above table, it becomes evident that there is no tool that can perform all the functions required. What.Hack is excellent in generating scenarios; however, it lacks some aspects such as a Unity 3D environment, customization of difficulty level, and integration into learning systems. OfficeGuard contains an office environment tailored to students, which lacks adaptation, provides little feedback, and fails to cater for requirements of large corporations. ForenSEEK is an application that utilizes unity and serious games; however, it focuses on forensics rather than phishing. PhishGuard solves most problems identified in one single design. PhishGuard stands out because it incorporates solutions for all five challenges faced by other applications. The use of PhishGuard is straightforward. The PhishGuard application appears to have all the qualities of the tool needed for phishing needs.

VII. DISCUSSION

PhishGuard is a system that brings together three elements that cannot be found together anywhere else.

• a realistic business environment

• individualized training according to individual roles

• integration within current business systems

The people who made PhishGuard used Unity to build it and this is a good choice according to studies by ForenSEEK and Lockedout. These studies show that Unity is a platform for creating serious games. The way PhishGuard teaches people is based on methods that are shown to work in a book called what and on a capture-the-flag approach by Ahmed and other people. One big decision the people who built PhishGuard made was to use something called Scriptable Objects to create scenarios. This means that people who make security content can write scenarios without having to know how to program which's really important for companies. In the organizations involved in such activities, it is the responsibility of the security personnel, and not the developers, to ensure that the scenario content is kept current. Using the concept of Scriptable Objects and Streaming Assets ensures that new scenarios could be developed as soon as there are new phishing schemes without necessitating the processes of building and redeploying the application. There is another component of PhishGuard known as the Indicator-Level Feedback Subsystem. A phishing tool known as Phish Guru highlighted the importance of providing feedback following failed attempts, but what PhishGuard does differently is providing feedback on deception strategies and their explanations in relation to fundamental social engineering principles. The method of teaching adopted by PhishGuard corresponds to the principle of cognitive load, which indicates that instructional material should be provided at the time of engagement and relevance. The PhishGuard tool has another element known as xAPI analytics pathway, which is an organizational feature. This pathway lets security teams gather data from the organization, which helps them identify departments that need training. It also helps link training results to world phishing susceptibility and generate evidence for compliance with regulations like ISO 27001 NIST CSF and GDPR Article 32. There are some limitations to PhishGuard, including:

- The initial role-profiling relies on employees reporting their roles.
- In the future it might be possible to use inference from Active Directory attributes or HR system integration.
- The current design does not address SMS phishing or voice phishing.
- The effectiveness of the NPC system, which is used for priming has not been tested.
- The QR-code and multi-day spear phishing scenarios are planned for development, which means PhishGuard will be more effective, in the future and will be able to teach people about PhishGuard and how to avoid phishing tactics.

PhishGuard is a tool that can help people learn about PhishGuard and how to avoid phishing tactics. It is an important tool for companies to use to protect themselves from phishing attacks and to learn about PhishGuard.

VIII. CONCLUSION

This paper is about PhishGuard, a training platform for corporate employees to learn about phishing. PhishGuard is a game that uses Unity to make the training more fun and interesting for employees. The people who made PhishGuard looked at tools and found some problems. These problems are that there is no way to simulate a corporate environment the training is not personalized for each employee there is not enough feedback it does not work with other corporate systems and it does not cover all the different types of phishing that are happening now.

PhishGuard has five parts that work together to solve these problems. These parts are an office environment, a system that creates different phishing scenarios, a way to make the training harder or easier based on the employee's performance a way to give feedback and a way to track how well the employees are doing. The people who made PhishGuard used ideas from successful games and training platforms such as ForenSEEK, Lockedout and OfficeGuard. They also used practices for making games and training platforms.

The plan is to test PhishGuard and see how well it works compared to training methods. In the future the people who made PhishGuard will add scenarios, such as smishing and phishing with QR codes. They will also make it possible for employees to work together as a team to respond to phishing attacks. PhishGuard will be an useful tool, for corporate employees to learn about phishing and how to protect themselves. PhishGuard is a training platform that will help corporate employees learn about PhishGuard and how to avoid phishing attacks.

REFERENCES

[1] Verizon, "2024 Data Breach Investigations Report," Verizon Business, 2024. [Online]. Available: https://www.verizon.com/business/resources/reports/dbir/

[2] IBM Security, "Cost of a Data Breach Report 2023," IBM Corporation, 2023. [Online]. Available: https://www.ibm.com/reports/data-breach

[3] A. Kovacevi˘ c and S. Radenkovic, "SAWIT—security awareness im- provement tool in the workplace," Applied Sciences, vol. 10, no. 9, p. 3065, 2020.

[4] K. Khando, S. Gao, S. M. Islam, and A. Salman, "Enhancing employees information security awareness in private and public organisations: A systematic literature review," Computers Security, vol. 106, p. 102267, 2021.

[5] J. Hamari, J. Koivisto, and H. Sarsa, "Does gamification work?—a literature review of empirical studies on gamification," in Proc. 47th Hawaii Int. Conf. System Sciences, 2014, pp. 3025–3034.

[6] M. Silic and P. B. Lowry, "Using design-science-based gamification to improve organizational security training and compliance," Journal of Management Information Systems, vol. 37, no. 1, pp. 129–161, 2020.

[7] Y. Ahmed, M. Ezealor, H. Mahmoud, M. A. Azad, M. B. Farah, and M. Yousefi, "Enhancing security awareness through gamified approaches," arXiv:2404.09052v1 [cs.CR], Apr. 2024.

[8] D. Dicheva, C. Dichev, G. Agre, and G. Angelova, "Gamification in education: A systematic mapping study," Journal of Educational Technology Society, vol. 18, no. 3, pp. 75–88, 2015.

[9] M. E. Pantaliano, M. C. R. Blanco, A. N. M. Rabano, J. D. C. Co, H. B. Villaalba, A. A. R. C. Sison, and C. J. Centeno, "ForenSEEK: Gamifying learning experiences in digital forensics using Unity Engine and augmented reality technology," in Proc. IEEE Int. Conf. on Computing (ICOCO), 2024, pp. 196–201.

[10] M. Kostic and I. Savelji´ c, "Interactive cybersecurity awareness: Creating´ a gamified password strength checker with Unity," in Proc. 15th Int. Conf. on Business Information Security (BISEC'2024), Nis, Serbia, Nov.˘ 2024.

[11] P. Kumaraguru, J. Cranshaw, A. Acquisti, L. Cranor, J. Hong, M. A. Blair, and T. Pham, "School of phish: A real-world evaluation of antiphishing training," in Proc. 5th Symp. Usable Privacy and Security (SOUPS), 2009, pp. 1–12.

[12] Z. A. Wen, Z. Lin, R. Chen, and E. Andersen, "What.Hack: Engaging anti-phishing training through a role-playing phishing simulation game," in Proc. CHI Conf. Human Factors in Computing Systems, 2019, pp. 1–12.

[13] O. BenAoumeur, "OfficeGuard: The anti-phishing training game," Honors Thesis, Univ. at Albany, State Univ. of New York, May 2024.

[14] T. Denning, A. Lerner, A. Shostack, and T. Kohno, "Control-AltHack: The design and evaluation of a card game for computer security awareness and education," in Proc. ACM SIGSAC Conf. Computer Communications Security (CCS), 2013, pp. 915–928.

[15] S. Singh and A. Kaur, "Game development using Unity game engine," in Proc. 3rd Int. Conf. Computing, Analytics and Networks (ICAN), IEEE, 2022.

[16] G. Lampropoulos and A. Sidiropoulos, "Impact of gamification on students' learning outcomes and academic performance: A longitudinal study comparing online, traditional, and gamified learning," Education Sciences, vol. 14, no. 4, p. 367, 2024.

[17] R. Fatima, A. Yasin, L. Liu, and J. Wang, "How persuasive is a phishing email? A phishing game for phishing awareness," Journal of Computer Security, vol. 27, no. 6, pp. 581–612, 2019.

[18] M. H. Phan, J. R. Keebler, and B. S. Chaparro, "The development and validation of the Game User Experience Satisfaction Scale (GUESS)," Human Factors, vol. 58, no. 8, pp. 1217–1247, 2016.