Leveraging UX-Centered Design in Cybersecurity: A Case Study of Developing a Cybersecurity Awareness Training Web App

Supervisors: Dr. Beran Necat & Dr. Nawaz Khan

Student Name: Muhammad Qasim

Student ID: 12687766

University of Essex (Online)

ABSTRACT

This research centers on the development of a cybersecurity awareness training web app, grounded in a UX-centered design framework. The research employs a Systematic Literature Review (SLR) methodology, analyzing 1605 studies from 2012 to 2024. After applying inclusion and exclusion criteria, 16 studies were selected. Key theoretical models, including the Technology Acceptance Model (TAM), Protection Motivation Theory (PMT), and Unified Theory of Acceptance and Use of Technology (UTAUT), are used to frame the analysis, alongside empirical studies demonstrating the effectiveness of UX-centred approaches. The web app is designed to improve employee cybersecurity awareness and mitigate insider threats by applying key principles of user experience (UX), such as usability, cognitive load reduction, and gamification. Findings reveal that, as a core artifact of the research, the web app serves as a theoretical case study that demonstrates how UX frameworks can be practically implemented to create engaging, intuitive training modules. While real-world user testing is not part of this study, the app's design reflects the operationalization of UX principles aimed at fostering sustained behavioral change in users. The research contributes to the growing body of literature on the application of UX in cybersecurity training and presents the web app as a functional tool to enhance cybersecurity awareness within organizations. The research concludes on the fact that the web app developed in this research represents one of the practical usages of the UX-centered framework on cybersecurity awareness training. Those core principles of UX will be integrated in the application-developed aspects such as user engagement, simplification of information, immediate feedback, and behavior reinforcement-that show how theoretical ideas are articulated into a tool that functions in real life by calling for better cybersecurity behaviors.

Keywords: UX-Centered Design, Cybersecurity Awareness, Gamification, Behavioral Change, Insider Threats, SLR

Table of Contents

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

UX	User Experience
MFA	Multi-Factor Authentication
TOTP	Time-based One-Time Password
UI	User Interface
IT	Information Technology
CBT	Computer-Based Training
AI	Artificial Intelligence
CI	Continuous Improvement
LMS	Learning Management System
PMT	Protection Motivation Theory
TAM	Technology Acceptance Model
UTAUT	Unified Theory of Acceptance and Use of Technology
CLT	Cognitive Load Theory
HCI	Human-Computer Interaction
GDPR	General Data Protection Regulation

CHAPTER 1: INTRODUCTION

1.1. Background and Problem Statement

1.1.1. Cybersecurity and the Human Element

In this modern, digitized world, cybersecurity breaches have become one of the most critical concerns for organizations, whatever their size (Hughes et al., 2024). With every advancement in technology, though, systems have grown strong and impregnable from outside attacks. As different industry reports suggest, human error causes about 90% of data breaches. Simple negligence in this respect includes clicking on phishing links or using weak passwords (Billman, 2024). More complex behaviors involve deliberate bypassing of its protocols or leaking sensitive information. Most of organizations implement different advanced technical mechanisms to secure data-such as firewalls, encryption, and multi-factor authentication (Malinina, 2023).

All these security mechanisms can easily be bypassed if the employees dealing directly with the sensitive information or handling it are not aware of cybersecurity. For instance, if an employee fails to recognize a phishing email or utilizes the same password between accounts, there will be an increased risk associated with the breach even if the deployment of different security systems is made. Therefore, one of the most important ways to minimize insider threats and ensure organizational resilience has become the enhancement of cybersecurity behavior in employees.

1.1.2. User Training and the Role of UX

Because of such vulnerabilities, many organizations start implementing cybersecurity awareness training programs (Van Steen & Deeleman, 2021). Such training is supposed to give insight to employees about common security risks and best practices and the importance of following security policies, but traditional methods usually are not very effective at engaging users. Traditional cybersecurity awareness programs often rely on static, text-heavy content or repetitive, lecture-style delivery methods that do little to build meaningful motivation for long-term behavior change. According to Lindgren (2020), UX-driven frameworks save the day. UX design is the practice of improving the way people interact with a product or system to make that interaction more intuitive, engaging, and effective.

In current study, therefore, try to fill the existing gap in cybersecurity awareness training by building a web application informed by the UX-centered design framework (Silic & Lowry, 2020). The application is intended to operationalize principles of UX that will bring about engaging yet effective training to reduce human error and insider threats within organizations. The value of this

research study lies in the theoretical and practical explanation of how UX design can be used to develop this app for cybersecurity awareness and behaviors among employees.

1.2. Research Aim & Objectives

1.2.1. Research Aim

The primary aim of this research is to develop and present a cybersecurity awareness training web application that demonstrates the practical application of a User Experience (UX)-centered design **framework**. The web app serves as a case study that operationalizes key UX principles such as engagement, cognitive load reduction, real-time feedback, and behavior reinforcement to enhance the effectiveness of cybersecurity training (Gunduz & Das, 2020). This project focuses on bridging the gap between theoretical frameworks and practical applications by creating an artifact that can improve user behavior and mitigate insider threats in cybersecurity.

1.2.2. Research Objectives

- To **identify** how user experience (UX)-centered design principles can be leveraged to develop effective security awareness programs that improve employee cyber hygiene and reduce insider threat vulnerabilities.
- To **evaluate** the key factors that influence the effectiveness of UX-centered cybersecurity awareness programs in promoting sustainable behavioral changes among employees.
- To **assess** how the web app operationalizes the UX-centered framework to enhance user engagement and reduce human error in cybersecurity training.
- To **determine** how the web app serves as a practical artefact that bridges the gap between UX theory and its application in cybersecurity training.

1.2.3. Research Questions

- How can organizations leverage user experience (UX)-centered design principles in crafting security awareness programs to improve employee cyber hygiene and reduce insider threat vulnerabilities?
- What are the key factors influencing the effectiveness of UX-centered cybersecurity awareness programs in promoting sustainable behavioral changes among employees?
- How can the web app operationalize the UX-centered framework to promote user engagement and reduce human error in cybersecurity training?
- How does the web app function as a practical artefact that bridges the gap between UX theory and its application in cybersecurity training?

1.3. Contribution of the Artefact

The primary contribution of this research is the development of a cybersecurity awareness training web app that serves as both a theoretical and practical artefact (Barendse, 2023). This web application represents the operationalization of key UX-centered design principles, providing a real-world example of how these theoretical frameworks can be applied to enhance cybersecurity awareness and reduce insider threats within organizations.

1.3.1. Theoretical Contribution

At the conceptual level, the web app is based on the principles of UX design, studied since high-end intellectual fields but still poor in infotainment in cybersecurity training. Casual cybersecurity awareness initiatives have often failed in meaningful engagement of users, with users becoming average passive learners, with an inability for long-term behavioral transformation (Bitrián et al., 2024). The artifact developed in this research is an effective example of the practical application of a UX-centered approach to improve user experiences in the cybersecurity training domain.

This web app overcomes inefficiencies in traditional training methodologies by applying crucial UX design principles to minimize cognitive load, engage users, provide immediate feedback, and reinforce behavior (Yigit et al., 2024). Every design decision for the app has been informed by theory in UX to create intuitive and engaging interfaces that ease complex information into actionable insights, bringing long-lasting change to the user's behavior (Faith et al., 2024).

The theoretical framework for the study is the UX-centered cybersecurity design framework, which stipulates considerations for the design of user-centered systems to reduce cognitive overload and ensure fun engagement techniques, such as gamification, that enhance motivation (Yigit et al., 2024). In that respect, the web app embodies these principles and shows how they might be implemented in practice.

1.3.2. Practical Contribution

The online tool is more than an intellectual exercise; it is a practical artifact developed to demonstrate what the principled operationalization of UX might look and feel like within cybersecurity training environments (Faith et al., 2024). Each of the stages of the UX-driven framework-user engagement, simplification of information, real-time feedback, and reinforcement of behavior-is consequently baked into the design of the app, which makes it a rich case study in realizing these concepts in practice.

1.3.3. User Engagement

The onboarding process itself greets its users by gently leading them through instinctive and smooth processes for logging in with ease and minimum cognitive load. This increases their comfortability with the system. The app instantly provides feedback to users immediately after taking quizzes or interactive exercises (Li et al., 2019). Although this web application does not rely on natural users' feedback for improvements or testing in this research, it is an effective artefact in bringing into light the practical application of UX principles (Faith et al., 2024).

The background, objectives, and contributions of this research, which is focused on the development of a UX-centered cybersecurity awareness web application, were outlined in Chapter 1. It also introduced the research aims and objectives, together with the theoretical and practical contributions of the project. Chapter 2 discusses the relevant literature, considering basic principles of UX, what theoretical frameworks and behavioral change models are present, and can be applied to developing any effective cybersecurity training application.

CHAPTER 2: LITERATURE REVIEW

2.1. UX-Centered Design

User Experience (UX) design has become a cornerstone in creating effective applications, especially in fields where user engagement and comprehension are critical. In cybersecurity training, UX principles are increasingly important because it ensures that users learn about security concepts and apply them in their daily tasks. The next section describes the basic UX design principles such as usability and the Cognitive Load Theory, and it examines the appropriateness of these for developing an effective cybersecurity training application.

2.2. Theoretical Framework

Based on theoretical frameworks, such as the Technology Acceptance Model, Protection Motivation Theory, and the Unified Theory of Acceptance and Use of Technology, the web application's design is strongly informed. These models were supportive to the design of GUI; establishing easy to manage interface, in terms of TAM and motivational security strategies for PMT. The real-time feedback option with an added fun and games aspect which has been integrated into the app will enhance the user's acceptance while at the same time fostering long term behavior change in accordance to the UTAUT model.

2.2.1. Technology Acceptance Model (TAM)

One of the most popular and well-proven frameworks explaining how users accept and use any particular technology is the Technology Acceptance Model (1989). TAM assumes two major factors influencing an individual's decision to adopt and use new technology: perceived usefulness and ease of use, as shown in Figure 1 (Ebot, 2024). Whereas perceived usefulness is the degree to which an individual believes that using a particular system would enhance their job performance, and perceived ease of use is the degree to which a person believes that using a particular system would not require an effort on their part (Dash and Ansari, 2022). In cybersecurity, TAM can be used to understand how employees have perceived UX-centred cybersecurity measures (Tam et al., 2022).

For instance, if the employees find that the cybersecurity protocols are easy to use and they believe these protocols protect their data and facilitate their work (Alderwood and Skinner, 2018). They are more likely to adopt and use them consistently (Alighieri, 2021). This is of special concern during the development of security awareness programs, which greatly depend on employee engagement and compliance (Gratian et al., 2018). TAM provides a useful lens to determine the

likelihood that these programs are accepted by the users they are designed to protect. (Baker et al., 2023).

Moreover, as TAM fundamentally deals with user perceptions, it is similar to the thinking behind the UX design process, which ultimately wants to make interfaces and experiences intuitively user-friendly and effective (Hasani et al., 2023). This research applies TAM to understand what critical factors would keep individuals from adopting UX-centred cybersecurity protocols and pinpoint areas where these protocols could improve see Figure 2 for technology acceptance Model.

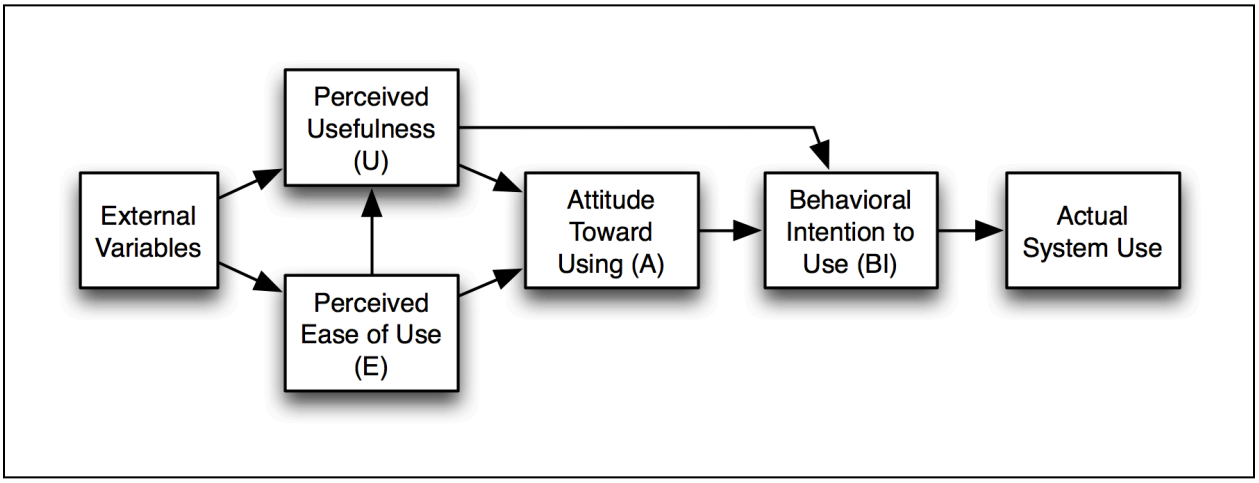

Figure 1: *Technology Acceptance Model*

Note: Taken from (Baker et al.2023)

However, TAM provides a valuable framework for assessing and improving the acceptance of UX-centred cybersecurity measures, ensuring that these protocols are technically robust but also user-friendly and effective in practice.

2.2.2 Protection Motivation Theory (PMT)

Protection Motivation Theory (1975), developed by Rogers, is one of the psychological theories explaining how people get motivated to engage in protective behaviors in the light of perceived threats (Seuwou et al., 2016). According to PMT, two major cognitive processes influence people's actions: threat appraisal and coping appraisal, as shown in Figure 2. Threat appraisal thus involves assessment of the severity of the potential threat and one's vulnerability to (Heierhoff and Choun, 2023). Consequently, as the theory holds, individuals are most likely to adopt protective measures when threat perception is high severity and high vulnerability and efficacy expectations regarding protection behavior and self-efficacy are high. PMT is applicable in cybersecurity, particularly in understanding how fear appeals, such as warnings on the consequences of security breaches, affect

employee behavior (Al-Zahrani, 2020; Tam et al., 2023). For example, if an employee knows the nature of data breaches that are both financially and reputably costly and also believes that adopting complex passwords or multi-factor authentication are effective means of preventing a data breach, then he/she is more likely to adopt protective behaviors (Seuwou et al., 2016). PMT supports designing security awareness programs that motivate employees to engage in protective behaviors. PMT can also be used to structure cybersecurity training programs to take advantage of both threat severity and response effectiveness components (McKenney, 2021). The figure 2 is a model of the Protection Motivation Theory, in which perceived severity, vulnerability, response efficacy, and self-efficacy influence threat and coping appraisals that will result in protection motivation and go on to health behaviors.

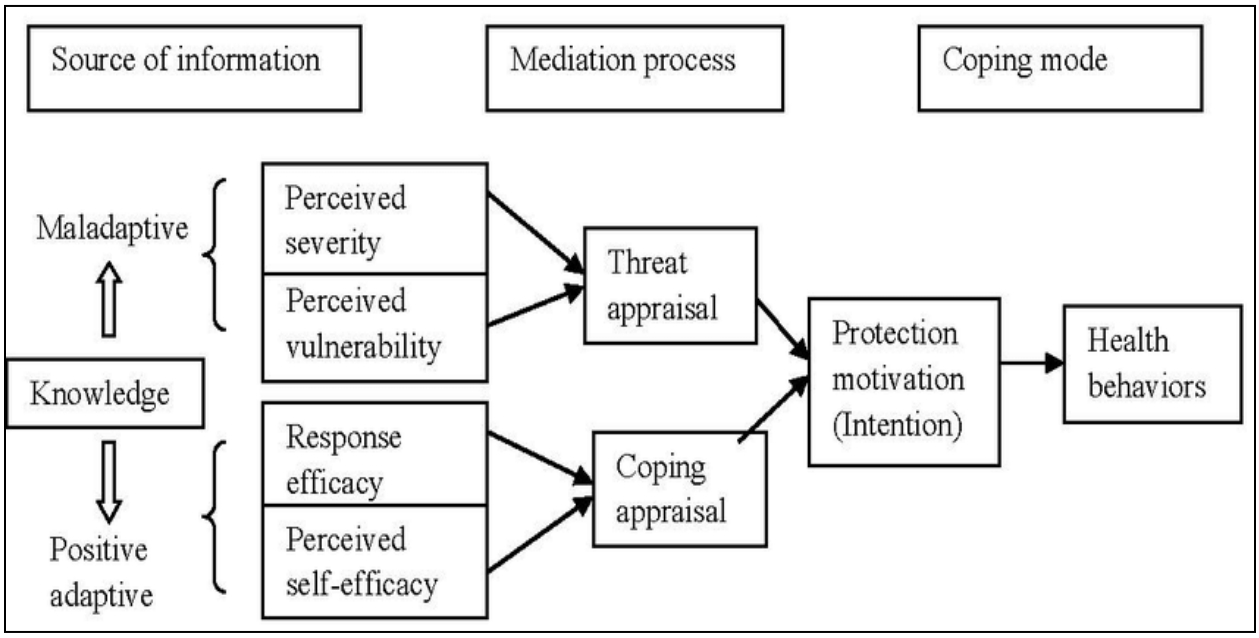

Figure 2: *Protection Motivation Theory*

Note: Taken from (Heierhoff & Choun 2023)

PMT thus offers a handy framework for constructing security awareness programs that spur protective behaviors. If designed with variables of threat severity, vulnerability, and self-efficacy in mind, then the program can become very instrumental in actively engaging workers with cybersecurity practices, hence reducing the risk of security breaches (Seuwou et al., 2016).

2.2.2. Unified Theory of Acceptance and Use of Technology (UTAUT)

The Unified Theory of Acceptance and Use of Technology is a broad model that defines how users reach acceptance and further use technology in its integrity. Developed in 2003 by Venkatesh et

al., UTAUT recognizes four major factors that play a role in the acceptance of new technologies: performance expectancy, effort expectancy, social influence, and facilitating conditions (Feth et al., 2017). This research is an aid in nailing down factors that, aided by UTAUT, most influence employee acceptance of up-to-date, UX-centred cybersecurity tools at the workplace. One would also require facilitating conditions that would include access to training and technical assistance, making one at ease feeling competent and confident in using such tools. Figure 3 illustrates the UTAUT model of the Unified Theory of Acceptance and Use of Technology by showing performance expectancy, effort expectancy, social influence, and facilitating conditions that influence behavioral intention to affect use behavior.

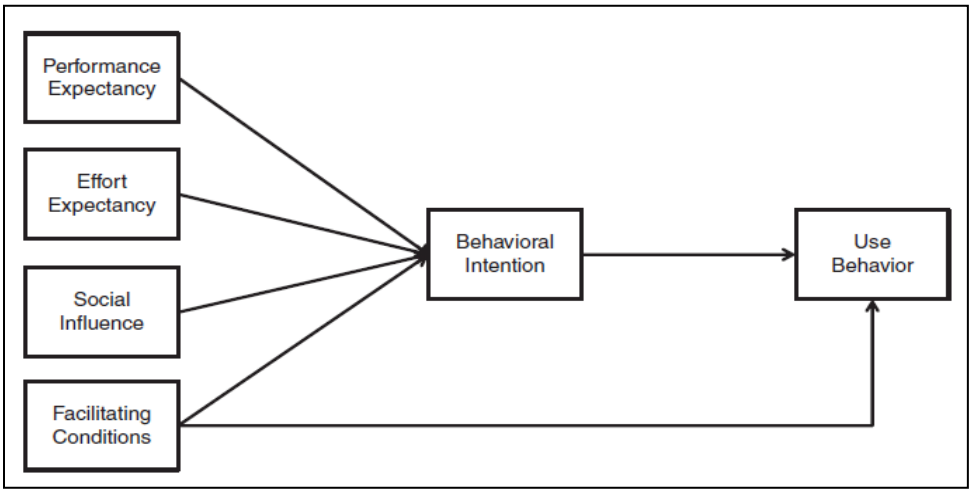

Figure 3: *Unified Theory of Acceptance and Use of Technology*

Note: Taken from (Malinina,2023)

Considering these factors, UTAUT comes into the spotlight as a means of explaining how to develop and introduce cybersecurity programs that are not only technically sound but also widely accepted and effectively used by employees in general for better security (Feth et al., 2017). These theoretical models, namely TAM, PMT, and UTAUT, are strong in providing an understanding of the factors that influence the adoption and usage of cybersecurity measures.

2.2.3. Cognitive Load Theory in Cybersecurity Applications

Cognitive Load Theory maintains that an individual has a finite capacity for processing novel information and that overload impairs knowledge retention and a reduction in understanding. Sweller's Cognitive Load Theory, (1988), differentiates between three types of cognitive load: intrinsic, extraneous, and germane. During UX design for cybersecurity training, the only burden of relevance is to decrease the extraneous cognitive load. The modules should avoid complications

that are not necessary, including navigation that might confuse people, too much text, or irrelevant information altogether. According to Sweller et al. (2011), reducing extraneous load may be able to lead to better learning outcomes because it means that users are allowed to focus their efforts on processing and understanding the essential information (Zwilling et al., 2022).

2.2.4. Relevance to Cybersecurity Training Applications

Other design keystones for cybersecurity training applications involve usability and Cognitive Load Theory. Norman (2013) says good design makes applications more usable but also extends to influencing user behavior by making the right actions obvious through design cues in cybersecurity applications, this would be about constructing the training modules in a way that they do not just present information to the users but guide them toward secure practices through well-designed interactions. The major application of usability and Cognitive Load Theory, UX-centered design principles, is considered most appropriate for successful performance in cybersecurity training applications.

2.3. Behavioral Change Theories

Theories of behavioral change are essential in the understanding of how users will interact with cybersecurity training tools, and underlying them will be the basis upon which those interactions can become permanent changes in user behavior. Regarding cybersecurity, training programs should not just educate the users but simultaneously bring about changes in their behaviors against insider and human error threats. Some of the key behavioral science theories covered here are Cognitive Load Theory and Engagement Theories, among others, to explore ways these theories are put into practice in the design and LADO of cybersecurity training applications.

2.3.1. Cognitive Load Theory in Behavioral Change

As it has been argued, CLT, suggested by Sweller (1988), draws her vitality from how managing the cognitive capacity of users promotes good learning outcomes.

2.3.2. Engagement Theories and User Motivation

Engagement theories are important, particularly in terms of user motivation, for behavioral change in cybersecurity. One of the widely acknowledged theoretical frameworks on this topic is the Self-Determination Theory or SDT-a motivational theory that splits motivators into intrinsic and extrinsic sources. Ryan and Deci (2000) observed that intrinsic motivation arises when one engages in an activity because the activity itself is inherently interesting or enjoyable, whereas

extrinsic motivation arises as a function of external contingencies, such as badges or even certificates.

For instance, gamification elements-that is, leaderboards and rewards-can enhance user participation and connect with the users' inner motivations. Simultaneously, extrinsic rewards-meaning badges for completing cybersecurity tasks, like enabling MFA offer positive reinforcement, and encourage further behavior modification. Hamari et al. (2014) argue that gamification, apart from the increase in engagement, may further influence feelings of accomplishment, which could lead to long-term behavioral changes**.**

2.3.3. Applying Behavioral Change Theories in Cybersecurity Training

The cybersecurity training should aim at changing the user's behavior, applying principles of Cognitive Load Theory and Engagement Theories. Thus, by lessening cognitive load and increasing the motivation of users, training can be provided for long-term adoption of secure behaviors. Norman (2013) has emphasized that effective design can promote certain actions and habits through cues and feedback principle directly applying to the cybersecurity training interfaces.

2.4. Gamification in Cybersecurity

Gamification in cybersecurity is a technique whereby game design elements, such as rewards, badges, and leaderboards, are used to implement user participation and motivation to ensure secure behavior. By embedding both the desire for mastery and personal satisfaction-motivators and extrinsic badges and rankings-these techniques foster active participation in cybersecurity training. Immediate feedback and rewards are the most facilitating to behavior change, according to behavioral models such as Fogg's Behavior Model, where gamification will play a motivator and trigger for secure practice. These nowadays are implemented practically in cybersecurity apps to give users not only an opportunity to learn but to apply their knowledge, balancing theoretical insights with practical challenges and outcomes.

Gamification of cybersecurity training utilizes both intrinsic and extrinsic motivators, such as mastery, badges, and leaderboards, to enhance user engagement in secure behaviors. According to Fogg's Behavior Model, the convergence of motivation, ability, and triggers-rewards, for example about behavior change.

As Deterding et al. (2011) have pointed out, intrinsic motivation in gamification is driven by users' desires for mastery, achievement, and personal satisfaction, whereas extrinsic motivation is

provided by the concrete rewards, such as badges or rankings in leader boards linked to immediate gratification for the completion of specific tasks or the demonstration of particular skills. Grounded in behavioral science, Hamari et al. (2014) showed that rewards provided directly after the completion of a task improve the motivation of users to engage with the training material, eventually changing behavior in the long run. Rewards in badge format act as positive reinforcement. Fogg's Behaviour Model, (2009), further develops these mechanics by stating that behavior occurs from the convergence of three factors, namely motivation, ability, and triggers.

2.4.1. Sustaining Behavioural Change Through Gamification

Long-term cybersecurity training success requires users to retain and apply knowledge. Gamification aids in this process by setting goals and rewarding systems that keep users continuously engaged in the process. Instead of having one learning curve, gamified training could be designed to offer periodic incentives to keep users coming back for more.

2.5. Cybersecurity Awareness and Human Behavior

Human behavior plays a critical role in cybersecurity is at once the weakest link and the first line of defense against breaches in organizational assets. As Hadlington bluntly points out, individual actions- susceptibility to phishing attacks, poor password conduct, or lack of attention to security updates- remain key contributors to the vulnerability of an organization.

However, cybersecurity is not a pure technical issue; human Vak alleged responsibility in the crime. A Verizon study of (2021) estimated that about 85% of data breaches included human involvement, via phishing, social engineering, or the stealing of credentials.For instance, employees use weak passwords or reuse passwords across different platforms to avoid the anxiety of having to remember different passwords, even when they know the risk. Dinev and Hart (2006) also assume that most of the users are not motivated to comply with safe policies even when those policies are known.

2.5.1. Addressing Human Factors Through Cybersecurity Awareness Training

To effectively address the human factors in cybersecurity, awareness training must go beyond simply disseminating information. It has to invoke a change in the behavior of users so that they realize the impact of their actions on security outcomes and are equipped with the ability to avoid common pitfalls. According to Sasse et al. (2001), security awareness training should be designed to make security behaviors habitual and easy to adopt. Training programs should mirror real-life situations that users are most likely to be involved in, such as phishing emails or suspicious links.

This approach applies the situational awareness concept spearheaded by Endsley (1995)-which has emphasized the need for users to understand their environment and the potential risks they might incur.

2.5.2. Psychological and Cognitive Aspects of Cyber Security Behavior

Understanding the psychological and cognitive drive for cybersecurity behavior is important to develop effective awareness programs. These biases make a user in cybersecurity either neglect warnings or fail to take precautions, such as setting up MFA or regularly updating software. As such, the TPB by Ajzen (1991) also offers meaningful insights into cybersecurity behavior. According to the theory, individuals are driven to act by their attitudes, perceived behavioral control, and subjective norms. According to Furnell and Thomson (2009), positive reinforcement and recognition of good security behavior are far more likely to create longer-term changes in the behavior of the workforce.

2.5.3. The Importance of Continuous Awareness Training

In this regard, awareness in cybersecurity matters cannot be one-off but ongoing to keep users well-informed and alert. Continuous training allows users to stay aware of emerging threats like ransomware or spear phishing attacks, understand how to protect them and protect the organization. Individual factors such as job role, age, and prior experience with technology were found to influence on the way users perceive and react to cybersecurity risks, according to research conducted by McCormac et al. (2017). In this regard, tailoring training to user groups will enhance its effectiveness by ensuring relevance and engagement across the board for all employees.

2.6.The Web App as a Practical Application

The web application developed in this research represents the practical embodiment of the UX-centered cybersecurity framework, translating theoretical principles into practical applications. In cybersecurity, where human behavior is often the weakest link, the use of a UX approach will better engage users and encourage them to adhere to security protocols.

2.6.1. Operationalizing UX Principles within a Web Application

The web application is therefore a case study in applying UX-driven design to better user engagement in cybersecurity training and security behavior. The application ensures intuitive navigation and clear instructions, minimizing cognitive load on users so they can devote more attention to the content of the training modules rather than to how to make their way through the platform.

2.6.2. Behavioral Reinforcement through Gamification

Among its many merits, one of the core features encompasses the use of gamification to reinforce secure behaviors. Werbach and Hunter (2012) have explained that gamification taps into human motivation through the utilization of game mechanics-like points, badges, and leaderboards-driving engagement to inspire behavioral modifications. For example, the app grants badges when mandatory tasks are completed, such as MFA setup or completion of a phishing awareness module. Indeed, as Hamari et al. (2014) note, gamification in learning environments increases user motivation, engagement, and participation-which is just so important during cybersecurity training.

2.6.3. The App as Continuous Feedback Loop

Another powerful principle of UX, which has been implemented in the web app, is that of feedback. As Shneiderman says, "Provide immediate feedback to interactions-critical to development of reinforcement learning habits that improve task performance", the implementation of real-time feedback mechanisms in the app shows every correct and wrong answer of the user for every quiz, along with explanations of answers in case one went wrong, instantly. In fact, according to Ajzen's (1991) Theory of Planned Behavior, this application's feedback should influence users in their attitudes and perceived behavioral control and intentions. However, the web app is the practical implementation of the UX-centered cybersecurity framework: usability principles, which will reduce cognitive load by including gamification and continuous feedback.

Moreover, Chapter 2 highlighted the theoretical underpinning that guides the design and development of UX-centered cybersecurity training applications: the Technology Acceptance Model, Protection Motivation Theory, and Cognitive Load Theory. Again, it pointed out the crucial role that gamification and behavioral change theories play in eliciting user interest and ensuring a long-term pattern of secure behaviors. The best basis for such practical application was given by those principles on UX in cybersecurity awareness training. The next section, Chapter 3, describes how those theoretical frameworks are operationalized in developing the cybersecurity awareness web application. This chapter primarily deals with how the subject of application design, application implementation, and testing has been carried out. Specific attention is given to how UX designs are integrated with gamification and feedback mechanisms to enhance user engagement toward long-term behavioral development.

CHAPTER 3: RESEARCH METHODOLOGY

3.1. Overview of UX-Centered Framework Implementation

The web application is developed on a UX-centered framework that places emphasis on user engagement, simplification of information, immediate feedback, and behavior change. These elements are crucial in making users more engaged with cybersecurity content to achieve usability and long-term behavioral change. Among the most important design principles that underpin this research is the Cognitive Load Theory, espoused by Sweller (1988), which argued that unnecessary cognitive load needs to be reduced so that learners can become attuned to learning. Thus, the web application is built with a minimalistic and intuitive interface; the login page, in particular, contains only the elements necessary for input, offering the opportunity for MFA. The typical trend that can be seen in the above example is gamification of engagement. These tools bring about intrinsic and extrinsic motivation through badges, and leaderboards, embedding secure behaviors into daily routines as suggested under Self-Determination Theory. According to Fogg's Behavior Model, after every quiz, the app actually gives feedback in real time, thus allowing the user to make amends then and there to reinforce positive behavior. Thus, this is a web app with stronger theoretical approach, and it will be very friendly to users as well as an effective tool for cybersecurity training.

3.1.1. Phase 1: User Engagement

The first stage of the framework entails user engagement, which is the core of participation in cybersecurity training. According to Costley and Lange (2017), this is best achieved by embracing intuitive design that fosters minimal friction in user experience. The web app uses visual elements such as badges and leaderboards, interacting with the users through quizzes and assessments by Pino et al. (2020). This is a strategy that engages users and also allows them to come back hungry for more, and to complete more training topics. This is very critical for creating long-term behavior change, as suggested by Muntean (2018), concerning cybersecurity practice.

3.1.2. Phase 2: Simplification of Information

The second critical stage of the framework is simplification in cybersecurity. Cognitive load theory, developed by Sweller (1988) and later elaborated in more recent studies, is used to manipulate information in chunks. Each of these modules is crafted concisely with visually engaging components, interaction, and other features that are congruent with findings from Wickens et al. (2019) on how cognitive overload reduction leads to better comprehension and

retention by users. According to Paas and van Gog (2019), well-structured content tends to enhance learning outcomes by reducing extraneous.

3.1.3. Phase 3: Real-Time Feedback

Real-time feedback is a key tenet within UX that facilitates immediate learning and behavioral correction of mistakes. According to Prinsloo and Slade (2017), real-time feedback is one of the core and integral features in learning platforms, enabling fast behavioral shifts and embedding learning iteratively. Thoms et al. (2018) demonstrate that immediate feedback enhances user motivation and is particularly effective at enhancing users' performance in training programs. In the web app, this feedback loop supports the user in tracing strengths and weaknesses regarding cybersecurity awareness, thus providing personalized learning.

3.1.4. Phase 4: Behavior Reinforcement through Gamification

The reinforcement stage is the last from the perspective of the framework proposed in this paper and is implemented using traditional elements of gamification. Badges and progress indicators are used to express rewards in the context of the web app that is developed through this thesis. Gamification should be used in training as it creates motivation for users in form of their possible levels of achievement. Gamification also recaptures positive behaviours when the user successfully completes training modules and answers the quiz questions. Hamari et al. (2019) noted that gamification is useful for promoting positive behaviour within the digital environment owing to extrinsic motivation rewards that make up gamification that act as motivation for continued interaction. These rewards help users of the web application to maintain secure behaviors for a longer time.

According to Koivisto and Hamari, (2019), behavior reinforcement through gamification indeed can achieve long-term behavioral change, especially in domains like cybersecurity, where continuous engagement and adherence to best practices are highly necessary. The application of badges and leaderboards in the app is therefore supported in the appropriate research as such instills a sense of achievement in its users and ultimately engages them in striving for continuous improvement of their cybersecurity skills Sailer et al. (2017).

3.1.5. Incorporating Theoretical Frameworks through SLR

This translation into a web app was informed by a Systematic Literature Review that highlighted critical theoretical frameworks in building a user-centered cybersecurity awareness framework. These, in providing the best avenues through which to enhance user engagement, lead to long-term

behavior change, and offer a human-centered design perspective. First, TAM, otherwise known as the Technology Acceptance Model, ranks in perceived ease of use and usefulness, which are two of the most vital components in user adoption. PMT was integrated into the web app using gamification techniques, such as badges and leaderboards, in combination with real-time feedback to further reinforce the consequences of poor cybersecurity practices.

These help to assess, respectively, performance expectancy, effort expectancy, and social influences through the UTAUT. The tracking of progress and feedback loops will make users stay tuned for a long period, hence assuring the app of long-term engagement. TAM, PMT, and UTAUT together played an important role in molding a user-driven motivational and efficient cybersecurity training app that promotes engagement in behavioral change.

3.2. Heuristic Evaluation Using Nielsen's 10 Usability Heuristics

A heuristic evaluation of the web application, based on Jakob Nielsen's 10 usability heuristics, was conducted regarding usability and user experience. This was meant to ensure the application met the set standards for usability; this would create an engaging experience and thereby enable more effective adoption of secure behavior. Feedback in the form of badges showing completed tasks reduces user uncertainty, thus motivating them. This again takes note of principles of Cognitive Load Theory by not wasting unnecessary mental resources, while re-enforcing feelings of control and achievement.

3.3. Artefact Development Process

The development of the web app was driven by the principles of the UX-centered framework, with a strong focus on user engagement, simplifying complex information, providing real-time feedback, and reinforcing secure behaviors through gamification. This process was iterative, with each phase of development designed to address specific user needs while ensuring that cybersecurity awareness training remained effective and user-friendly.

3.3.1. User Engagement: Login Page

The login page, as shown in Figure 4, is one of the most important features for engaging users right from the very beginning. Dombrowski et al. (2020) have pointed out that the first impression on digital platforms makes a huge difference in the user's motivation to continue using a system. In the web application, the design within the login page was performed in such a way that it would present minimal cognitive load, hence allowing users to get into the system without much hassle and wasting any time. Furthermore, MFA is integrated, which Saxena et al. (2021) point out is

indispensable in contemporary cybersecurity frameworks for protection against unauthorized access.

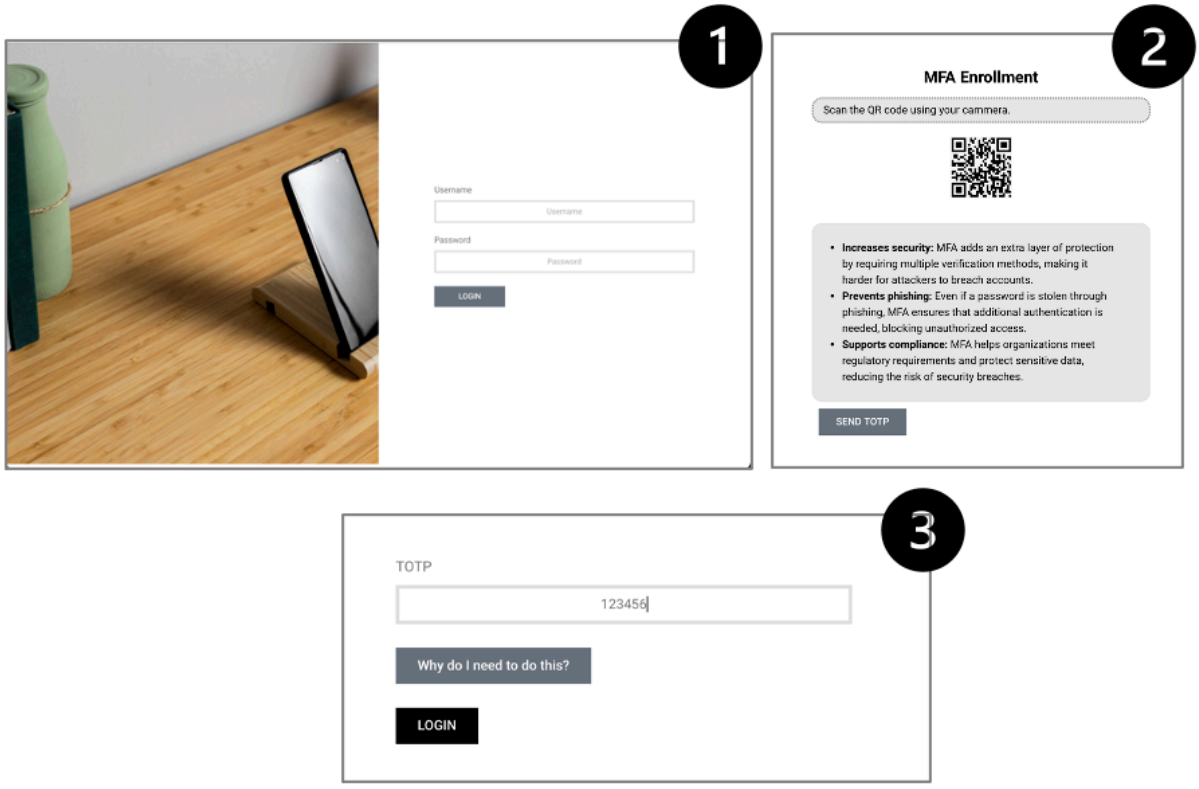

Figure 4: *User Login Page*

This Figure 4 shows the web app's login page, featuring a simple and minimalist design to reduce cognitive load. The use of Multi-Factor Authentication (MFA) enhances security by prompting users to send a Time-based One-Time Password (TOTP) after entering their credentials. Clear input fields and instructions minimize cognitive load. MFA prompt ensures enhanced security without complicating the user experience. Progress indicators show that the login process is moving forward, reducing anxiety for first-time users. The user-centered design approach here aligns with Muntean (2018), who argues that reducing friction in early interactions improves long-term engagement. The simplicity of the login page reduces initial user frustration, ensuring that users feel comfortable navigating the platform from the start.

3.3.2. Simplifying Information: Training Modules

The web app breaks down complex cybersecurity concepts into manageable and digestible modules. According to Sweller et al. (2019), cognitive load theory suggests that reducing

extraneous cognitive load is essential for effective learning. The web app applies this theory by presenting training materials in a clear, structured manner, using bite-sized content, short text, and Modular layout simplifies the complex subject of phishing by providing step-by-step instructions, as shown in Figure 8. Icons and images are used to explain concepts visually, supporting text and minimizing reading fatigue. Interactive elements, such as short quizzes embedded within the module, allow users to apply what they have learned immediately. As Costley and Lange (2020) note, multimedia content combined with active learning exercises improves retention and user satisfaction. The training modules in the web app embody this approach by offering a balance of text, visuals, and interactive quizzes, as shown in Figure 9. This method also addresses the need for simplifying cybersecurity information, ensuring users can understand and apply the concepts in real-world scenarios without being overwhelmed.

3.3.3. Real-Time Feedback: Feedback Screens

Providing real-time feedback is a critical element of the UX-centered framework. The feedback system in the web app is designed to deliver immediate responses to user inputs during quizzes and assessments. According to Thoms et al. (2021), real-time feedback can significantly enhance learning outcomes by helping users identify mistakes and understand correct answers immediately.

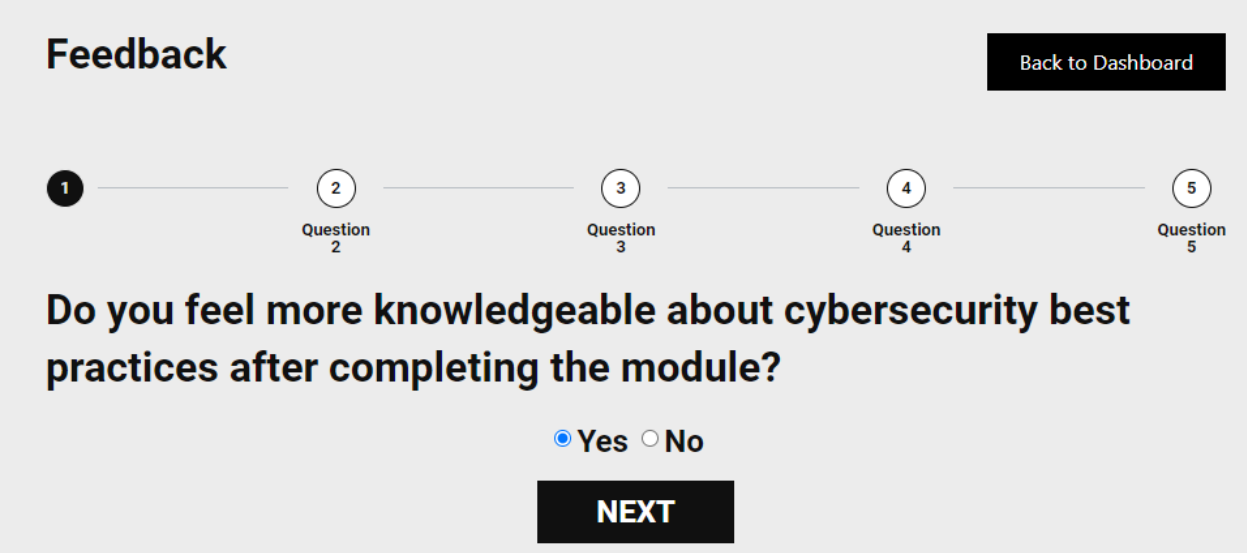

Figure 5: *Feedback Screen after Quiz*

Feedback questions are required as shown in Figure 5. The feedback system is an essential component in ensuring that users are constantly learning and improving (Nguyen and Ng, 2022). This real-time feedback loop is crucial for promoting continuous learning, which is vital in fields like cybersecurity where threats evolve rapidly.

3.3.4. Behavior Reinforcement: Gamification Elements

Gamification plays a key role in reinforcing secure behaviors by providing extrinsic motivation for users to engage with and complete training modules. The web app integrates badges, and a leaderboard system, which aligns with Hamari et al. (2019) findings that gamification increases user engagement by appealing to users' intrinsic desires for achievement and competition. All badges show users how much of the training they have completed, motivating them to reach 100%. A leaderboard encourages friendly competition, showing users how they rank compared to their peers. Rewards via badges, leaderboards, and other game-like elements of gamification create sustained behavior change, say Koivisto and Hamari. On the web app, these reinforce secure behaviors through visual recognition for user accomplishments for such actions as enabling MFA or advanced training modules.

3.3.5. Artefact as an Embodiment of the UX Framework

In this web application, throughout its development, the practical implementation of this UX-centered cybersecurity framework can be seen in every component, from a user-friendly login page through gamified, simplified training modules to real-time feedback. This approach is in full accordance with the principles discussed by Wickens et al. (2019) but also serves as an exemplary model that shall be followed by the rest of the cybersecurity training tools. As Pino et al. (2020) have pointed out, a good user experience is what makes users stick with training programs, even in a significantly critical area such as cybersecurity.

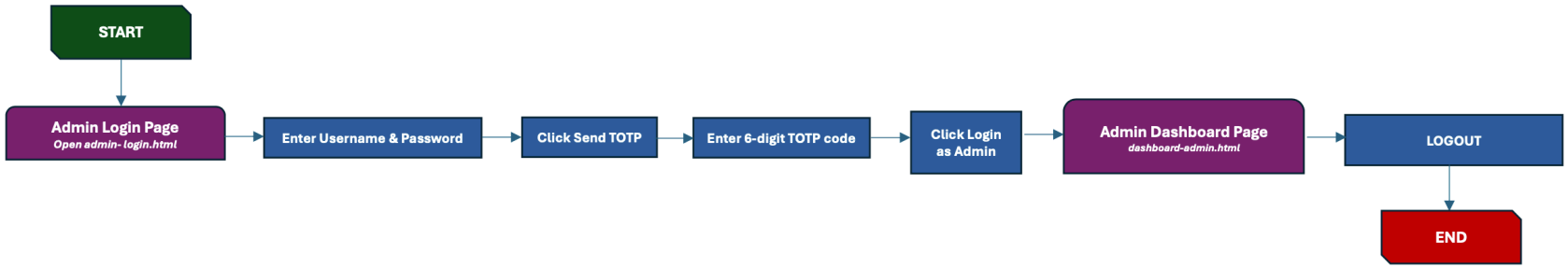

***Figure 6**: User Flow - Admin User*

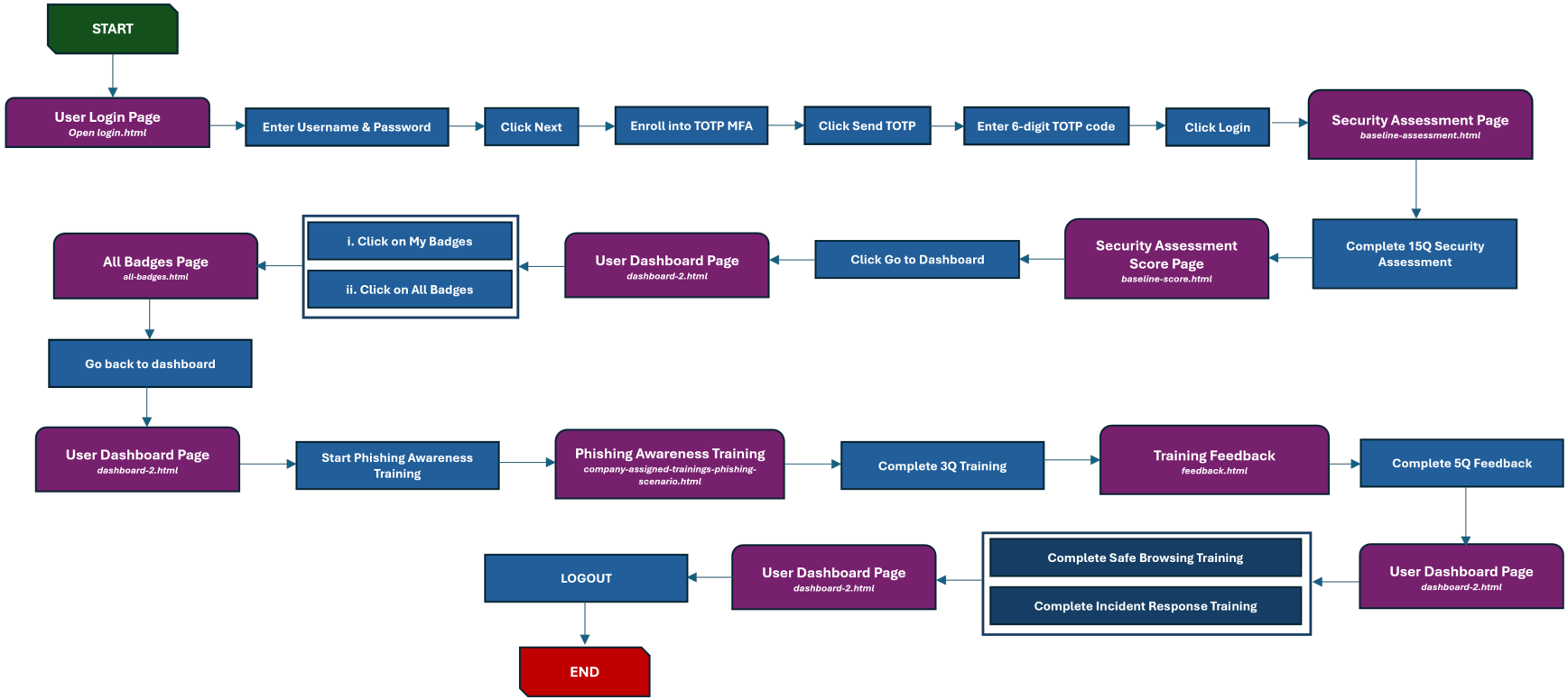

***Figure 7**: User Flow - End User*

Figures 6 and 7 represent flow diagram of a user and admin journey via the cybersecurity web app, starting from their respective login page. Thus, after credential inputs and TOTP MFA, the a user will undergo a security assessment, and then view the assessment score. A user will be taken to a dashboard where he/she can start the training, view badges, and finish three available trainings. An admin user on the other hand, will be taken to the admin dashboard to review training progress, feedback responses, and other metrics.

3.4. Artefact Implementation

The architecture of the web application accordingly follows a clear structure within the UX-centered framework: from the selection of the tech stack and design principles. To build this web application, WordPress would be an ideal option as a content management system due to its flexibility, ease of use, and wide support of plugins that enhance its functionality. WordPress was chosen for the present project given it maintaining scalability, and adaptability, and simplifies development. Elementor is used as one of the most popular page builders for WordPress to customize WordPress UI with a clean and responsive design that emphasizes usability.

3.4.1. Phase 1: User Engagement

User engagement is put at the forefront from the first interaction through a simple login page that has MFA integrated. This is developed with WordPress and customized using Elementor. Design principles are carried out based on minimalistic features, which reduces cognitive load and makes user onboarding frictionless. This clean interface is what sends an affirmative invite to your users for confident interaction with the platform, creatively setting the stage for active participation in the cybersecurity training modules.

3.4.2. Phase 2: Simplifying Information

The second layer of this UX-centered framework is a simplification of difficult information. These training modules, therefore, integrate icons, brief texts, and interactivity to deliver information in ways that limit cognitive overload. According to Mayer and Moreno (2017), new principles for multimedia learning can be very useful when implemented to simplify deep information. Practically, the design of the app helps users to remember and put into practice what they have learned. The guidelines of Sweller's (2019) Cognitive Load Theory are applied in the app's training modules by chunking content into smaller units that are easily handled by users to minimize the sum of mental effort required of them. It enhances learning because information is then processed and retained more effectively.

3.4.3. Phase 3: Real-Time Feedback

Another characteristic of the web application which directly relates to the third phase of the User-Centric Cybersecurity Awareness Framework is feedback. It is a conceptual framework of the web app under development which draws from concepts like user interaction, minimize cognitive load, real time feedback and behavior change through gamification. All of these elements are implemented in the web app that delivers the training in a way that is not only informative, but also engaging and motivating for the user to change the behavior in the long term.

Instant feedback is displayed to the user after every training module or a quiz that has been successfully done. The feedback system builds on introducing the correct solutions and also presents the typical wrong choices with descriptions of what the learner could do to avoid these mistakes. This mechanism of immediate feedback it is relevant to the work of Thoms et al. , (2021) who pointed out that real-time feedback is among the key factors for learning retention and allows users to correct mistakes while the information is still fresh in their memory.

Furthermore, there are performance summary tools on the application through which users can get to see how they are performing in various aspects of training. Saxena et al. (2021) have stated that more specifically, user feedback is a key aspect of UX design that is continuous, and this specifically helps engage the users and retain their interest in the completion of the training. This integrative concept guarantees that the web app not only provides information but also guides the users into becoming more security conscious on the use of the internet.

3.4.4. Phase 4: Behavior Reinforcement

The fourth phase of the UX-centered framework is reinforcement, and through gamification elements, the web application operationalizes this. Embedding badges and leaderboards will serve to execute all these to motivate users to undertake regular usage of proper interaction with training modules. Hamari et al. (2019) noted that gamification can significantly increase user participation by using the concept of intrinsic motivation for users, and hence the concept is applied on the web app, which greets the user for achievements, such as enabling MFA, completing any module, or having high quiz scores.

3.5. Operationalizing UX Principles

These web app features demonstrate specifics about how UX principles are operationalized in such a cybersecurity training context a reduction of cognitive load by simplifying interfaces to reinforce behavior through gamification. These components, in sum, translate UX theory into reality. Each

phase of this framework engagement, information simplification, real-time feedback, and behavior reinforcement was translated into actionable features within the app and ensured that the platform for improving cybersecurity awareness would be intuitive, effective, and engaging. Such decisions about design in the application are rooted in research by Koivisto and Hamari, which has argued that a combination of UX principles with gamification has much more effective learning experiences.

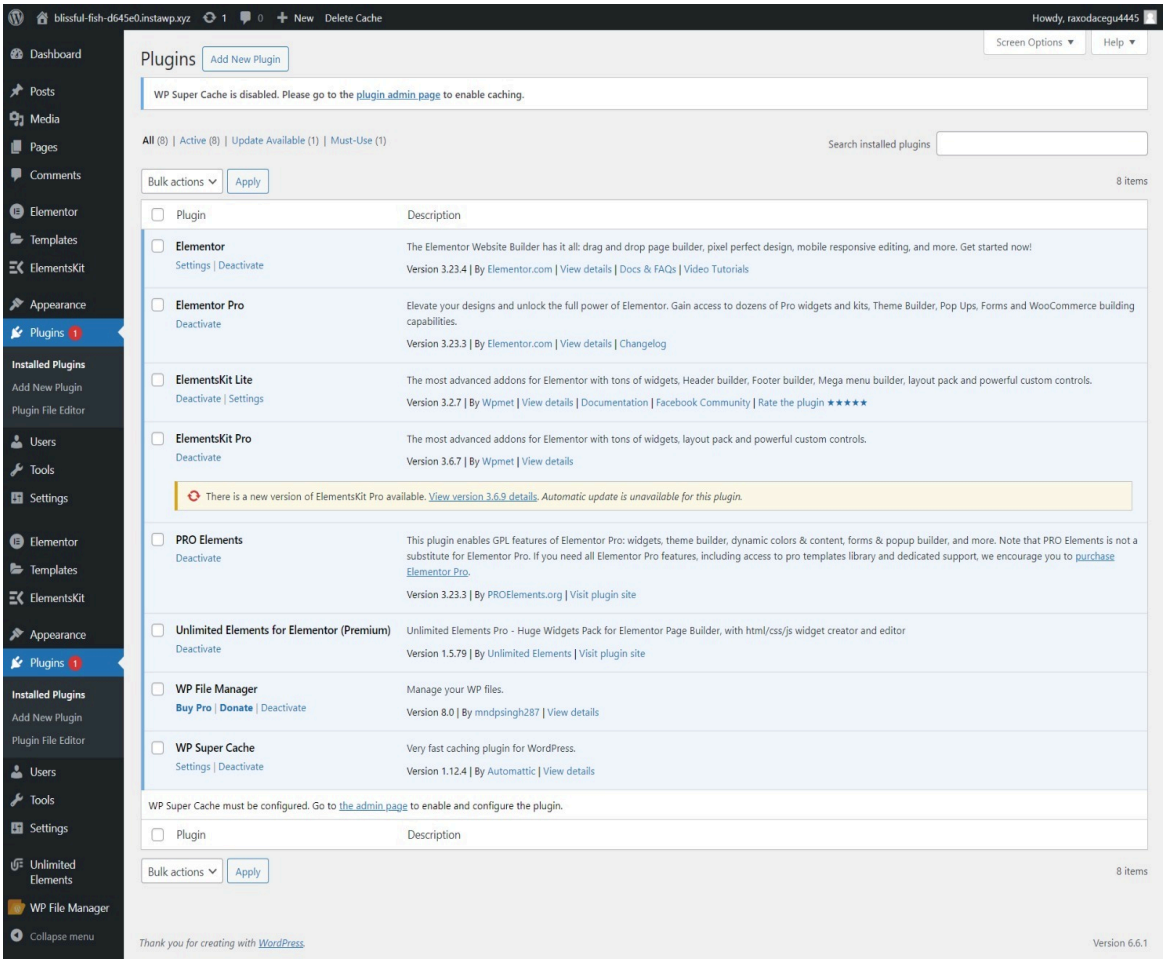

Figure 8: *Installed WordPress plugins supporting the web app's functionality and user engagement*

Figure 8 displays the list of installed WordPress plugins used in the web app development. Key plugins like Elementor**,** WP File Manager**,** and WP Super Cache enhance the app's design flexibility, file management, and performance.

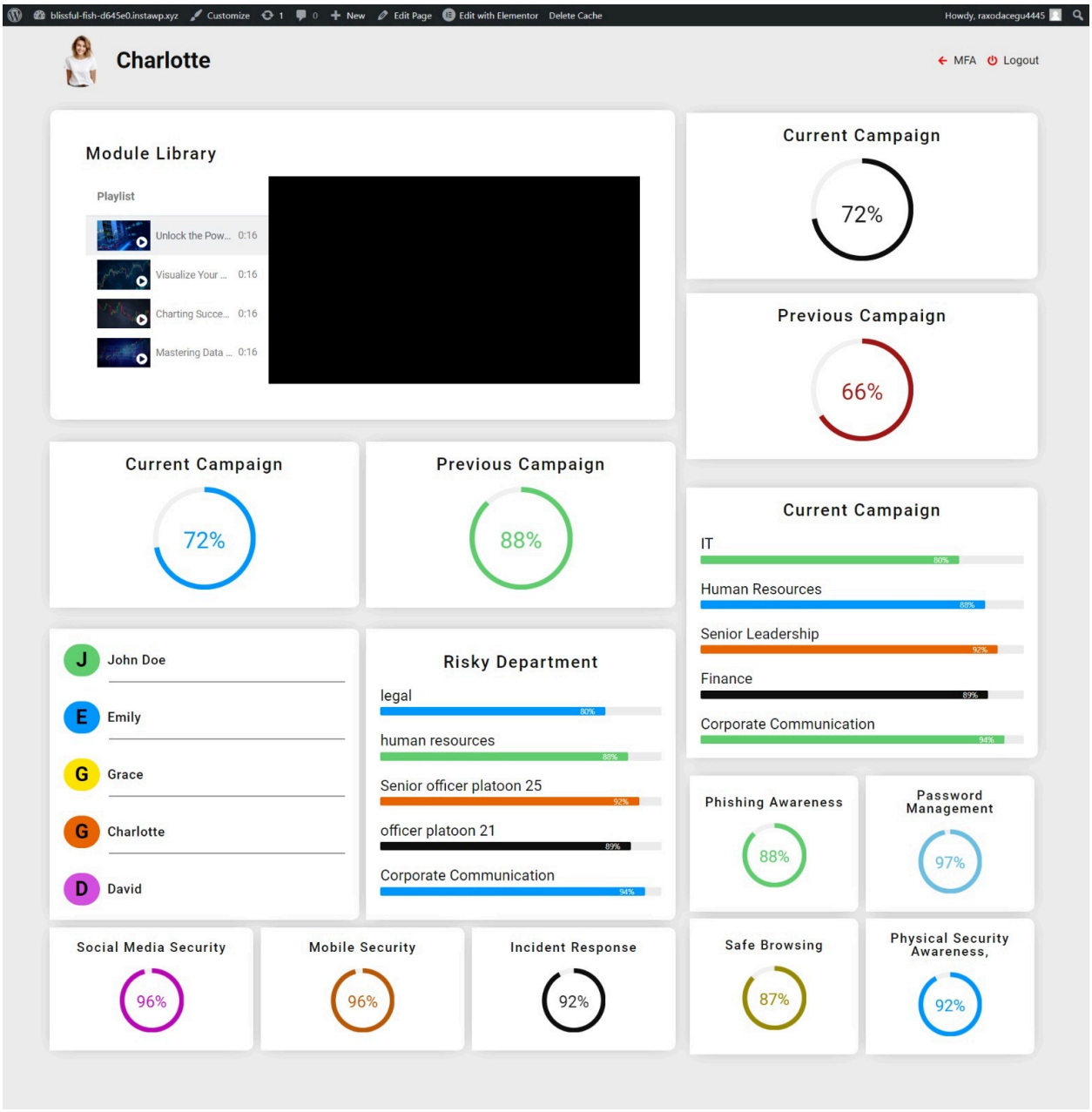

***Figure 9**: Admin dashboard showing user and department metrics for ongoing cybersecurity campaigns*

Figure 9 illustrates the admin dashboard in WordPress during development. Admin dashboard presents real-time data on current and previous cybersecurity training campaigns. The dashboard tracks user progress and departmental risks, displayed through interactive graphs and progress indicators.

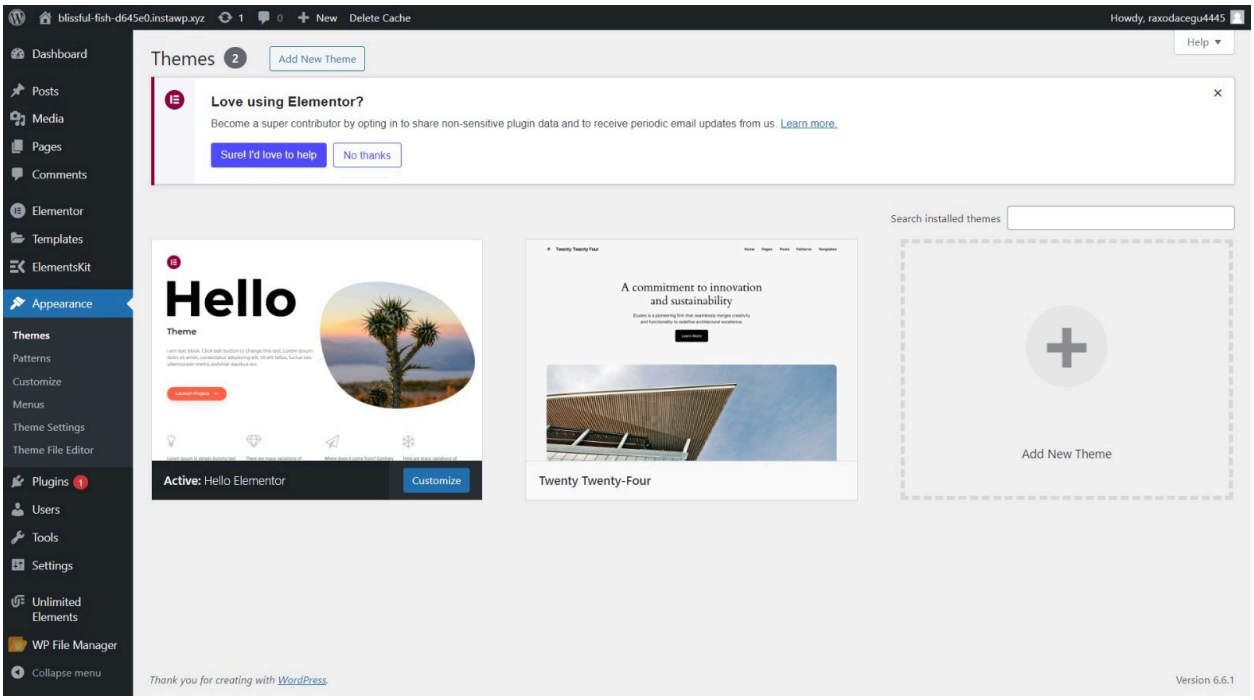

Figure 10: *WordPress theme selection, illustrating the active Hello Elementor theme used for the web app's design*

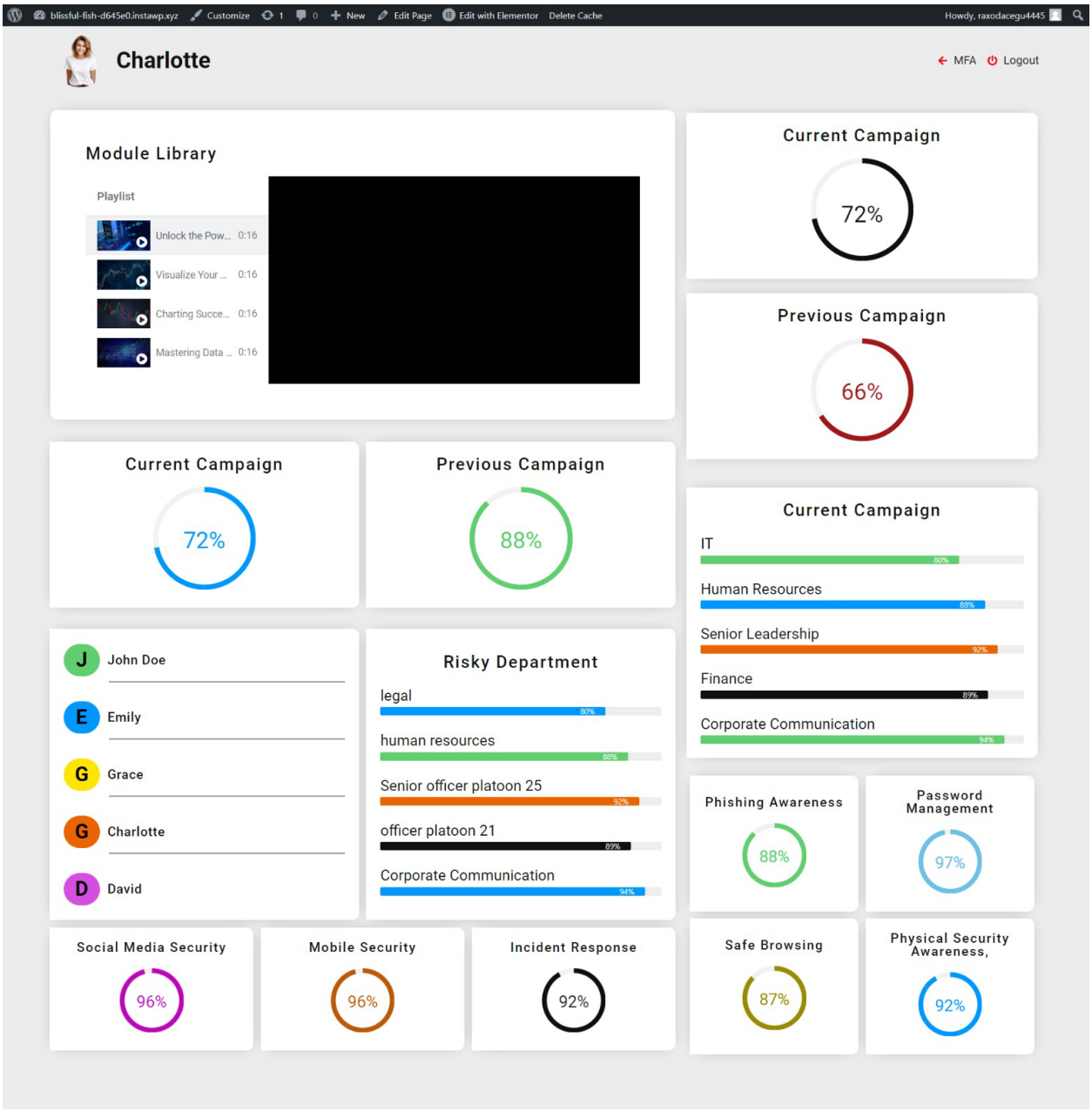

Figure 11: *User WordPress Engagement with UI of application*

Figure 10 shows the WordPress theme selection, illustrating the active Hello Elementor theme used for the web app's design. Figure 11 shows User WordPress Engagement with UI of application during development in WordPress.

Thus, Chapter 3 elaborated on the research methodology that guided the development and assessment of the UX-centered cybersecurity awareness web application. It presented a systematic process toward a feasible and effective tool in training people about cybersecurity, drawing on the bodies of knowledge within UX design, gamification, and behavioral science. The outcome of this

study will be reflected in Chapter 4, which shows the implementation of the performance in user engagement, behavior change, and overall effectiveness. The chapter continues with an analysis of data collected during the evaluation phase of the study to determine the impact of the UX-centered approach on cybersecurity awareness and the reduction of insider threats.

CHAPTER 4: FINDINGS

4.1. Theoretical Impact of UX Design on User Behavior

The key principles of UX-centered design for improving cybersecurity awareness graphed into better user behavior are reflected in the core of the web application developed within this research. The primary objective of the UX framework is to provide a seamless, engaging, yet effective user experience that would encourage users to maintain secure behaviors, thereby reducing cybersecurity risks like insider threats (Tatum, 2023). This can imply a theoretical alignment with UX principles that may influence user behavior in substantial ways, especially regarding engagement, learning retention, and long-term behavioral change.

4.2. User-Centered Design for Engagement

One of the core elements of UX design is being user-centered, and which means it should be designed around the needs and expectations of the targeted audience (Sharma, 2024). The given web application has been designed to implement a User-centred Cybersecurity Framework by easily and intuitively engaging the user, simplifying it, giving feedback, and reinforcing behavior. Regarding the user's engagement, the official interface has been simplified with game-like features such as badges or leaderboards, which keep users' interests alive for effective participation. In terms of simplification, the complex notions about cybersecurity have been reduced to simple and understandable modules that will lessen the cognitive overload and increase understanding. It instantly provides feedback after quizzes, thus allowing users to correct their mistakes immediately and reinforce learning. Finally, rewards in the form of badges for behavior reinforcement promote consistent engagement in securing behavior over the long term.

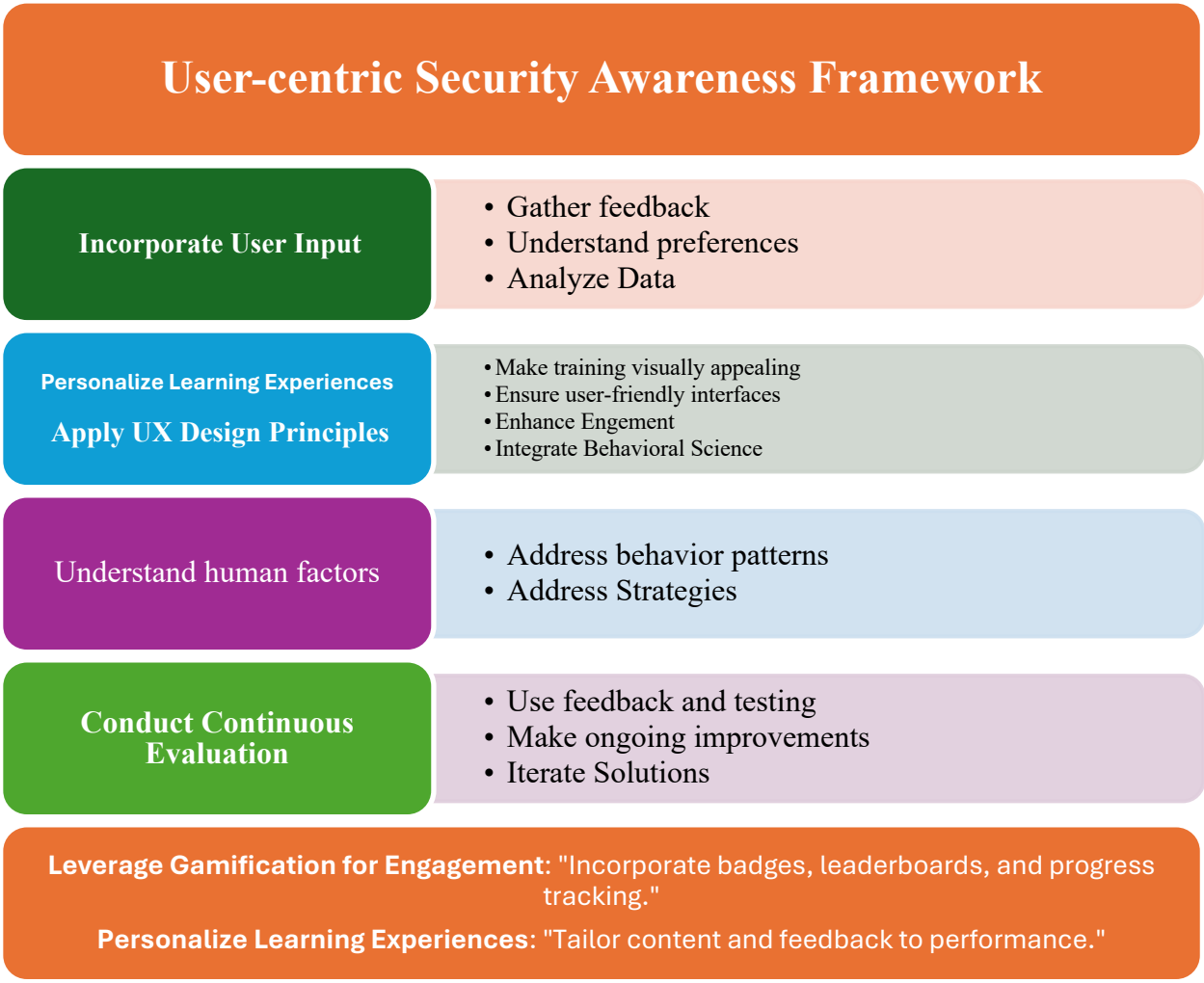

Figure 12: *User-Centric Security Awareness Framework*

Figure 12 represents the User-Centric Security Awareness Framework, which focuses on integrating user input, applying UX design principles, and behavioral science to enhance engagement in cybersecurity training. It emphasizes continuous evaluation through feedback and testing to refine solutions. Ultimately, the framework aims to improve security awareness, increase compliance, and reduce insider threats. On that note, research by Sweller et al. (2019) also indicates that when users navigate a platform with less mental load and with ease, they are likely to be deeply engaged, especially at the level now necessitated within learning contexts. Cognitive Load Theory by Sweller, 2019 commits to credo when reporting that information is better digested by learners in chunkable bits. Real-time feedback, Corrections on-the-spot

The application of real-time feedback represents another significant constituent in the UX design for this app (Martin, 2018). This feature has been considered to conform to the principles of UX

for interactive engagement and feedback loops, which have been argued by some to help consolidate positive behaviors and mistakes more effectively than delayed feedback can (Saxena et al., 2021). The theoretical models of behavior change, like the Operant Conditioning Theory, do explain that feedback provided in real-time helps users to correct their behaviors far quicker for improved performances over time (Liu et al., 2018). The immediate feedback within the web app not only enables immediate correction but also reinforces the appropriate behaviors that may lead to long-term improvement in cybersecurity practices.

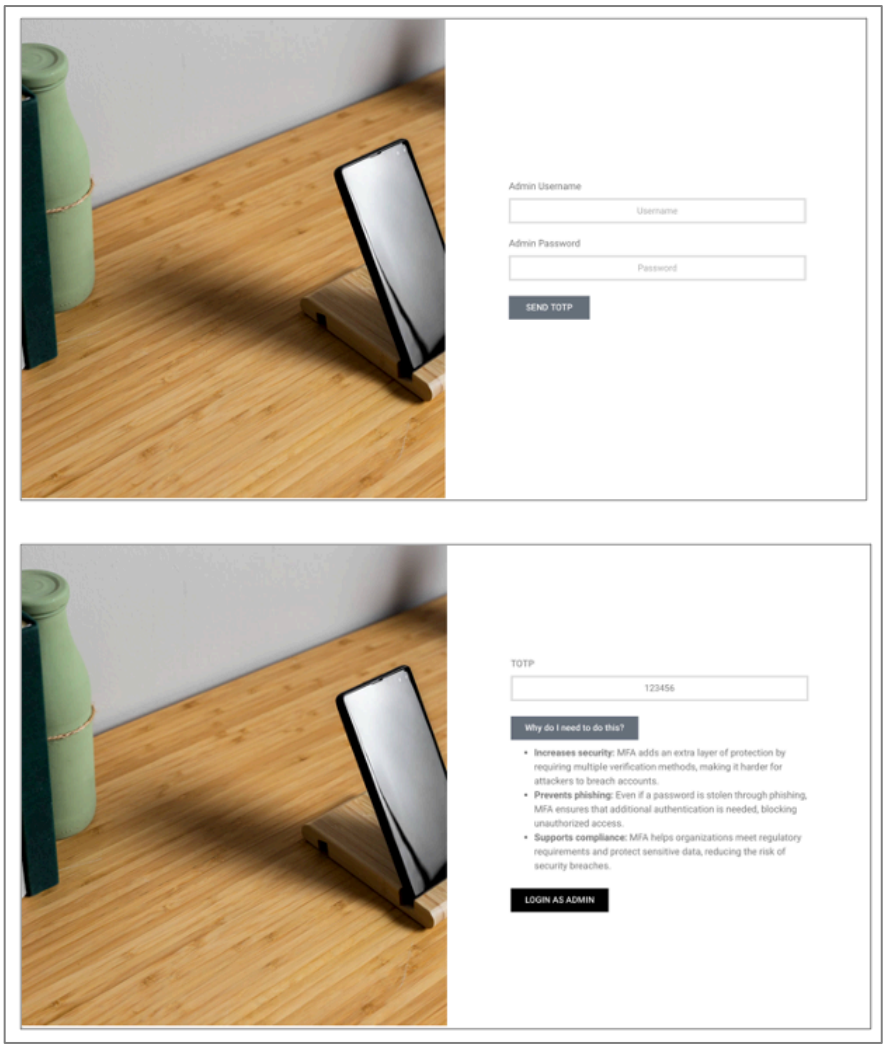

***Figure 13**: Login as Admin*

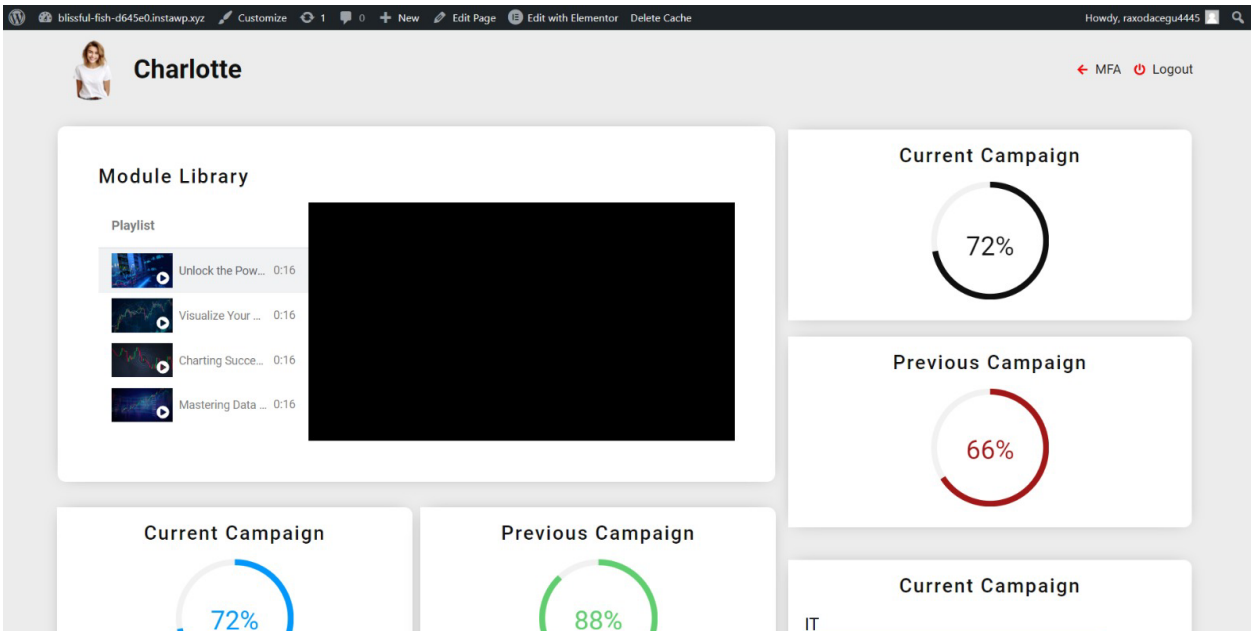

Figure 14: *Admin Dashboard Development in WordPress*

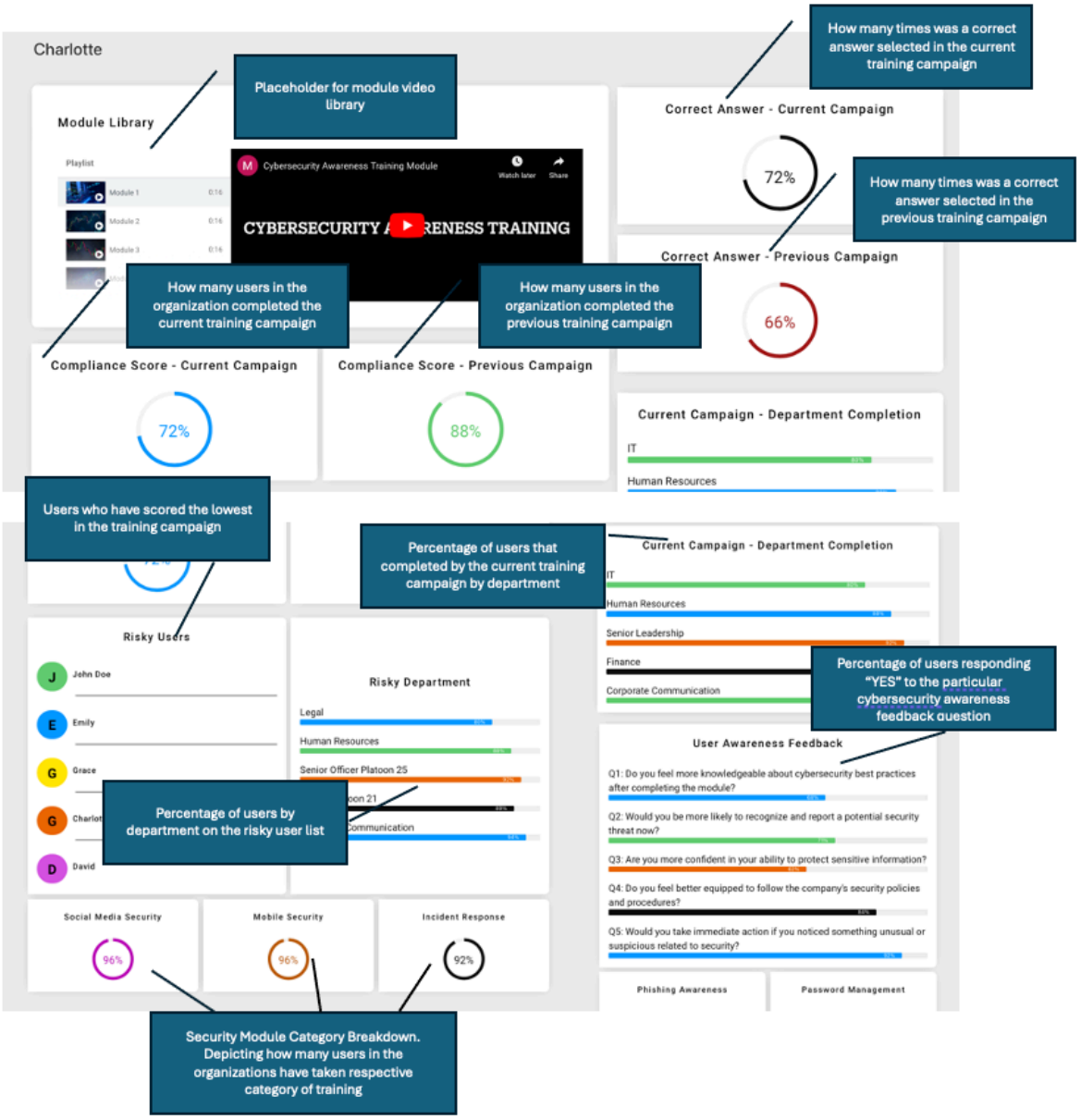

Figure 15: *Progress Data in Admin Dashboard*

Figure 13 depicts the administrative login interface, essential for secure access to backend functionalities. Figure 14 showcases the development of the Admin Dashboard within WordPress, highlighting customization and management features critical for system oversight. Figure 15 illustrates the purpose of each of the sections in the admin dashboard.

4.3. Gamification and Behavior Reinforcement

By embedding mechanisms such as badges, and leaderboards the web application taps into the UX principle of motivational design in encouraging users to complete training modules and apply their

learned knowledge. Hamari et al. (2019) proved that, indeed, gamification can be an effective tool in enhancing engagement and motivation in learning environments, especially when one sees their advancement and receives rewards for the same. This also aligns with the Behaviorist Learning Theory: positive reinforcement would lead to more sustained behavioral change. The studies by Sweller et al. (2019), Hamari et al. (2019), and Saxena et al. (2021) are among those that support the theoretical impact of UX principles on user behavior, demonstrating that well-designed, user-centered interfaces stand to lead to meaningful changes in behavior.

4.4. PRISMA Flow Chart

4.4.1. Development and Significance of the PRISMA Flow Chart

The flow diagram of PRISMA is a very critical artifact of this research that distinctively maps the filtration and selection process of studies included in the SLR ensuring transparency into all methodological rigor connected with its selection process (Homoliak et al., 2020). All decisional steps taken during the filtering and selection process of studies were explicitly drawn empirically through the diagram.

4.4.2. Process of PRISMA Flow Chart

The PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) flow diagram, as shown in Figure 16, visually represents the process of study selection in the Systematic Literature Review (SLR). The process consists of four key stages:

Identification: The initial search returned mainly from Scopus sources (n=1605). After the exclusion of sources irrelevant to the topic (n=300) and those excluded for other reasons, the total number of records reduced significantly for screening.

Screening: In the course of this stage, automation tools helped to mark 590 articles as disqualified based on predefined rules. After a detailed title and abstract scan, a further 544 irrelevant articles were removed, thus providing a more focused pool for in-depth review.

Eligibility: The full text of the 41 remaining articles was assessed for inclusion. Of the 27 that were excluded, these failed to meet certain study requirements by either not being representative of empirical data or falling outside the time frame of interest.

Inclusion: Ultimately, 16 studies were found to be appropriate for the review. More than relevant, these provided authentic views on the implementation of UX-centred design in cybersecurity awareness programs.

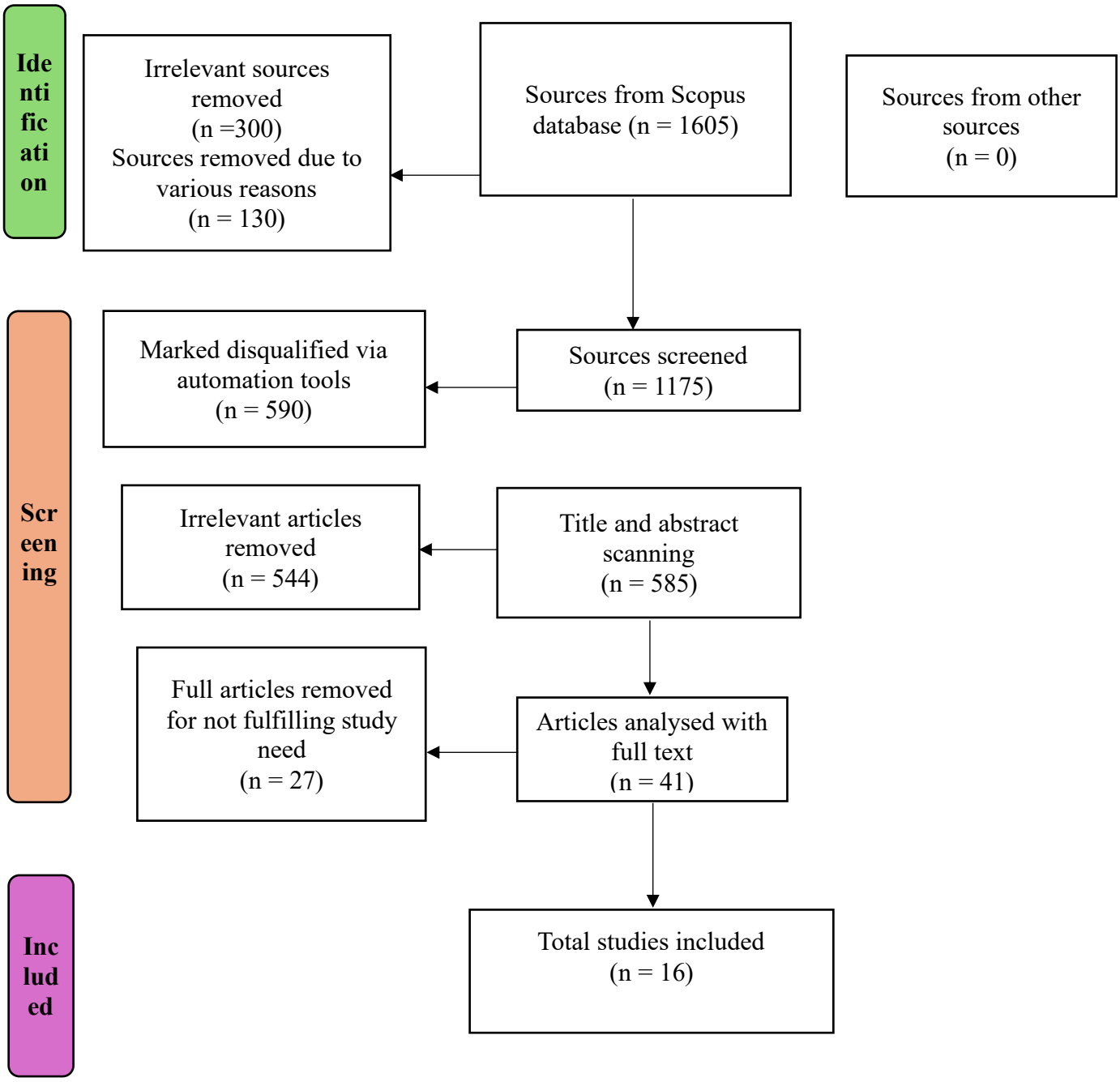

Figure 16: *PRISMA Flow Chart with Exclusion and Inclusion Criteria*

The element in presenting the detailed study of the selection process of studies, thereby underpinning the credibility and systematic nature of this applied Systematic Literature Review (SLR) methodology. Figure 16 describes by visuals every single step of the process of selection of a study, and it starts from the stage of identification, wherein the association of the database Scopus, 1,605 studies were originally taken into consideration. Further refinement is done in the screening stage, where automatic tools are used to exclude 590 articles based on set criteria, stressing that more detail was followed in the systematic and objective filtering process implemented in studying articles that remained relevant to the research questions. The eligibility phase represents a critical evaluation of full-text articles, 41 in total, out of which 27 were excluded for not satisfying the defined inclusion criteria for validation purposes of including only the best and most relevant quality of studies. This makes the PRISMA Flow Chart add to the credibility of the findings because it shows clearly that the results were from a very careful and well-structured review presented in Chapter 4.

4.5. Inclusion and Exclusion Criteria

4.5.1. Inclusion Criteria

The eligibility criteria in this research were meant to ensure that the literature sampled was relevant, of good quality and addressed the research questions. The systematic review targeted all peer-reviewed studies published from 2012 to 2024 to cover current trends in UX design integration within cybersecurity (Sarker et al., 2020).

4.4.2 Exclusion Criteria

The exclusion criteria were thus set to ensure the literature that would be identified as relevant and of good quality. In that respect, non-peer-reviewed articles were put out of consideration so that the studies reviewed would be of high academic standards (Sarker et al., 2020). After the application of inclusion and exclusion criteria, the research got 16 final papers, as shown in Table 1.

4.6. Systematic Data Analysis

4.6.1. Systematic Review Data Table

Table 1: *Systematic Review Data Table*

Sr#	Year of Publication	Country	Study Type	Objective	Methodology	Key Findings	Conclusion	Reference
1	2024	USA	Case Study	Exploring cybersecurity's impact on electronic health records (EHR) usage	SEM-ANN approach	Cybersecurity greatly impacts the use of EHRs.	Cybersecurity improves EHR performance in healthcare professionals.	Ala'a et al., 2024
2	2020	Saudi Arabia	Experimental Study	Evaluating gamification in cybersecurity awareness	Augmented reality game with 150 participants	Gamification enhances adherence to cybersecurity protocols.	Combining UX with gamification is effective in security awareness programs.	Alqahtani et al., 2020
3	2023	USA	Dissertation	Developing sustainable e-learning	TAM-driven approach	TAM enhances cybersecurity practices in e-learning.	E-learning platforms improve cybersecurity	Alquran, 2023

				platforms for cybersecurity			through TAM integration.	
4	2020	Saudi Arabia	Case Study	Integrating cybersecurity factors in e-government initiatives	IS success model	Cybersecurity improves IS success in e-government.	IS success is highly dependent on cybersecurity measures.	Al-Zahrani, 2020
5	2021	Saudi Arabia	Qualitative Study	Investigating cybersecurity attacks on academic data	Interviews	Education plays a mediating role in mitigating cyberattacks.	Higher cybersecurity education reduces academic data breaches.	Alibhai, 2021
6	2023	Jordan	Conference Paper	Integrating cyber security factors into Jordanian banks	TAM framework	TAM improves cybersecurity protocols in banking.	Integrating cybersecurity factors in banks boosts security adoption.	Baker et al., 2023
7	2021	UK	Case Study	Exploring cybersecurity in logistics	Review of case studies	Human factors influence cybersecurity in logistics.	Cybersecurity must focus on human behavior in	Cheung et al., 2021

							logistics settings.	
8	2014	Canada	Literature Review	Defining cybersecurity	Review of multiple sources	Provides comprehensive cybersecurity definitions.	Cybersecurity is a multi-dimensional concept with various factors.	Craigen et al., 2014
9	2016	South Africa	Conference Paper	Developing valid cybersecurity culture measurement	Mixed-methods research	Cybersecurity culture impacts organizational security practices.	Cybersecurity culture is critical for robust security systems.	Da Veiga, 2016
10	2022	USA	Survey	Assessing machine learning in cybersecurity	Review of existing machine learning studies	Machine learning aids in threat detection and prediction.	Machine learning is a critical component of future cybersecurity practices.	Dasgupta et al., 2022
11	2022	India	Experimental Study	Evaluating a cybersecurity training model	Qualitative interviews and surveys	Training models improve organizational	Effective training is key for enhanced	Dash et al., 2022

						security behavior.	cybersecurity awareness.	
12	2022	Belgium	Case Study	Understanding the relationship between cybersecurity perception and behavior	Mixed-methods study	Perceived knowledge of cybersecurity impacts actual security behavior.	Security awareness campaigns must target perception and behavior.	De Kempe et al., 2022
13	2021	India	Literature Review	Reviewing deep learning algorithms for cybersecurity	Analysis of deep learning studies	Deep learning effectively detects cybersecurity threats.	Deep learning will transform future cybersecurity frameworks.	Dixit & SilkAir, 2021
14	2023	USA	Survey Experiment	Evaluating factors that influence cybersecurity practices adoption	The Protection Motivation Theory (PMT) framework	PMT significantly influences cybersecurity practice adoption.	PMT is useful for designing cybersecurity awareness programs.	Dodge et al., 2023
15	2017	USA	Conference Paper	Investigating user-centered	Usability testing	User-centered security enhances	User-centered design is effective in	Doroftei et al., 2017

				design in cybersecurity		compliance with protocols.	improving cybersecurity practices.	
16	2024	USA	Dissertation	Exploring TAM for adopting cybersecurity in SMBs	Qualitative study	TAM adoption improves cybersecurity in small and medium businesses.	TAM is an effective framework for SMBs to adopt cybersecurity practices.	Ebot, 2024

4.6.2. User Engagement

These are major causes because user engagement is one of the key indicators of success for any cybersecurity training applications, and an engaging user interface is a potential motivator for users to complete training modules and absorb knowledge effectively to result in secure behaviors (Hadlington, 2018). Three key components are embedded into the dashboard: progress tracking, task list, and simplified menu Sweller et al. (2019). In this case, the app motivates users' interests because it fronts tasks and training modules and then organizes them into identifiable sections. Intuitive navigation, as suggested by Mayer and Moreno (2017), is an important component that sustains users' attention without frustration and hence increases engagement levels.

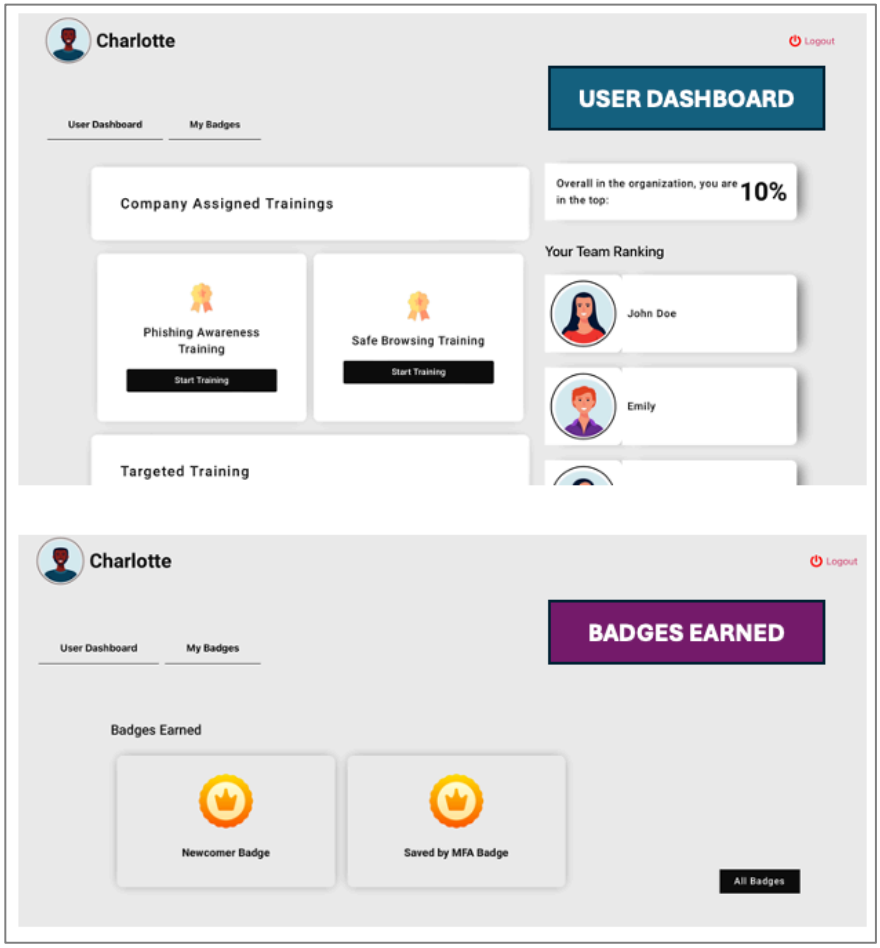

Figure 17: *User Dashboard Showing Clear Navigation and Task Progress*

Figure 17 shows the user's dashboard intuitively shows how users can engage themselves. Major elements such as navigation menus, badges earned, and clear task buttons remain highly accessible with ease. Such structure minimizes mental efforts and enhances engagement since users can easily

overview their training progress and tasks (Bada et al., 2019). Research has shown that the clarity of visuals in interfaces can boost user engagement because such clarity makes the task feel more doable and, thus, easier to access (Thoms et al., 2021). However, a factor that enhances user engagement is gamification, which is implemented in the dashboard. Long-term use of the app is created by giving users this sense of achievement using such gamified elements within the app. Hamari et al. (2019) explain that gamification proves to enhance user motivation and commitment to training tasks, which is highly required in cybersecurity education where consistent engagement is highly needed to instill secure behaviors. This further supports the assertion by Saxena et al., (2021), that immediate feedback forms a positive learning loop.

4.6.3. Simplification of Complex Information

Simplifying complex information is one of the key principles of successful learning, especially within a domain such as cybersecurity, which requires multiple technical and abstract notions that users need to master. The web app makes use of various aspects of Cognitive Load Theory in practice, whereby the learner would not be cognitively overloaded but instead could process and retain vital knowledge in cybersecurity. According to Sweller et al. (2019), the theory of cognitive load is underpinned by the notion that the aim of instructional design should be to minimize unnecessary load so that resources are freed to process essential information.

Figure 18 on the Training module on phishing awareness prepared to take students through the learning process in a significantly intuitive and non-scary manner. As Mayer and Moreno (2017) concluded, reducing the level of cognitive load results in an improvement in learning outcomes, which is possible by using multimedia elements, images, diagrams, and shorter text.

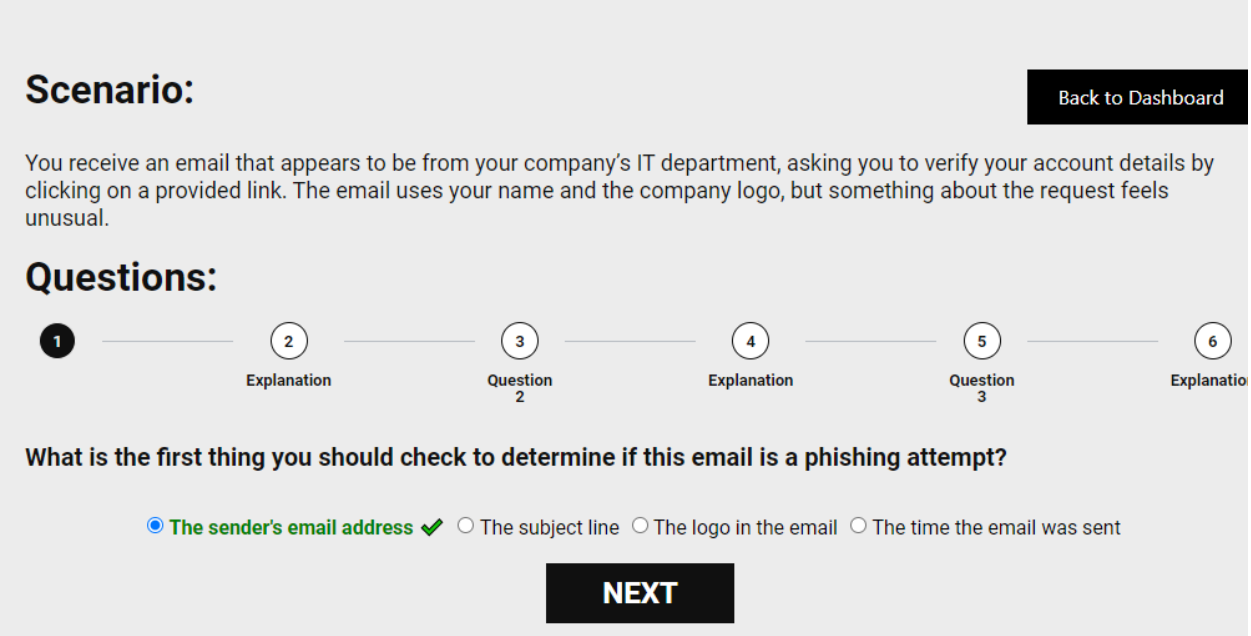

Figure 18: *Phishing Awareness Training Module Showing Visual Aids and Step-by-Step Instructions for Simplified Learning*

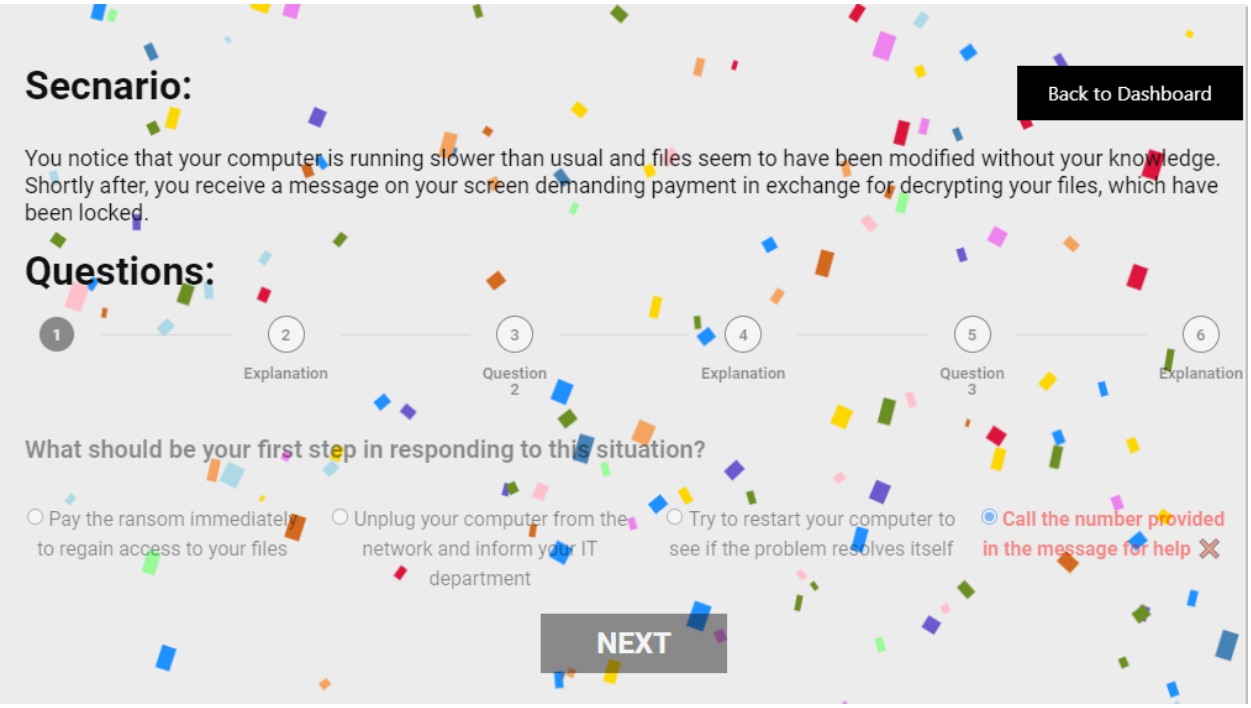

Figure 19*: Visuals at Different Steps*

Figure 19 represents a module developed for phishing awareness. As argued by Hamari et al. (2019), interactive learning methods have clear visual aids, icons, and step-by-step instructions that cut the topic into digestible parts; the accessible text and visual elements in the module help

break down complex concepts in cybersecurity. For instance, the phishing awareness module introduces a simple understanding of phishing and then progresses into other fine details, like how to identify phishing through emails. This layered approach is consistent with Sweller's Cognitive Load Theory, which posits that learning is optimized when information is presented in sequences that build upon prior knowledge.

4.6.4. Real-Time Feedback

The other significant constituent of this web application concerning cybersecurity is real-time feedback, which reinforces learning and changing behaviors. In this regard, immediate feedback will enable users to assess their understanding of the concepts in cybersecurity immediately after the end of a quiz or interactive module. Saxena, Kumar, and Goyal (2021) have clarified that through real-time feedback, learners will be able to instantly identify mistakes, which is one of the important attributes responsible for improving knowledge retention and ensuring long-term behavior modification. Figure 20 represents the feedback screen after a phishing awareness quiz. Notice that the feedback not only indicates what the user got right and wrong but also provides an explanation of why those answers were correct or wrong.

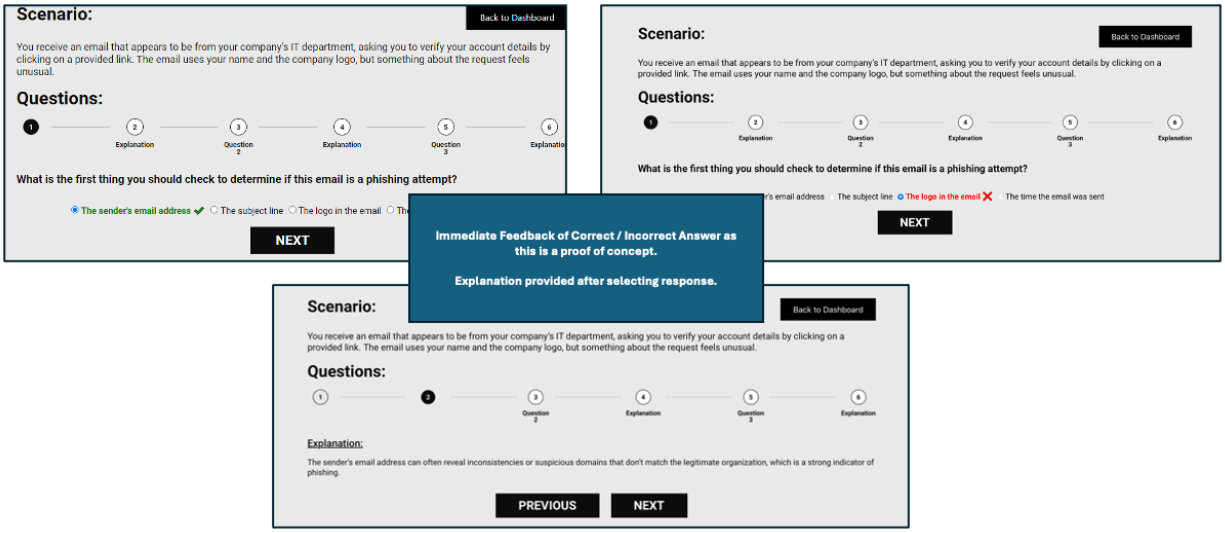

Figure 20: *Feedback Screen Displaying Correct and Incorrect Answers, Along with Explanation*

This aligns with Cognitive Load Theory, which suggests that learners benefit from clear guidance when processing new or complex information. Moreover, real-time feedback motivates them. Once users can see the results of their progress and be provided with feedback, they are most likely able to stick with the flow of training. This dynamic has been reaffirmed in the work of Hamari et al. (2019), while establishing real-time feedback, in particular, raises the level of motivation in

users if combined with gamification elements such as badges or progress indicators that further provide sustained engagement in learning environments.

4.6.5. Behaviour Reinforcement

Gamification elements, such as badges and progress indicators, are core to the behavioral reinforcement of the app, which in turn creates long-term engagement and sustains behavior change by creating a sense of accomplishment and continuous improvement. Badges are awarded to the users once they have gone through certain sections, such as once they have completed a module of training or they finished onboarding with MFA.

Badges and progress indicators employ the psychological principles of reinforcement, whereby users are made to repeat positive actions to get rewards. Hamari et al. (2019) reiterate that gamification in training environments can greatly improve user motivation with the inclusion of intrinsic and extrinsic rewards. Badges are visual representations of achievement that instill pride and a sense of progress, while progress indicators provide users with real-time feedback about their movement through the training program.

4.7.UX-Centered Cybersecurity Framework Flow

This section will introduce the flow of the UX-centered cybersecurity framework; it will explain how various design elements in the Web app directly contribute to cybersecurity awareness. Here, User Flow Diagrams for End Users and Admins can be employed to depict how design supports seamless navigation, learning retention, and long-term behavioral changes. The progress meters give a very good representation of their movement through the modules. According to Thoms et al., (2022) progress tracking is one of the core elements of gamification which will allow users to have their eyes on their objectives because it gives them a look at both how far they have come along and still have to do.

4.8.Gamification and Behavior Change

The purposeful approach of the web app is to raise user engagement and install safety behaviors, using gamification elements like badges, and leaderboards. With this, the system would apply the principles of behavioral science to create both intrinsic motivation by achieving and extrinsic motivation through tangible rewards consisting of long-term changes in cybersecurity practice. These gamification elements will be systematically integrated throughout the different phases within the users-centered cybersecurity framework; these will enable users not only to understand the concepts of cybersecurity but also apply them in practice.

Figure 21: *Gamification Elements Including Earned Badges and All Badges in the User Dashboard*

Figure 21 displays gamification features within the user dashboard, showcasing earned badges and all badges that visually tracks and motivates users' advancement through cybersecurity training modules.

Figure 22: *Earned Badges and All Badges in the User Dashboard*

Figure 22 displays the badges earned by users for completing cybersecurity training modules.

In conclusion, Chapter 4 presented the findings related to the implementation and performance of the UX-centered cybersecurity awareness web application. The results have identified how the integration of UX design principles, gamification, and real-time feedback is effective in engaging users and inducing behavior change. Chapter 5 will go on to evaluate some of the key web application features that are in development, namely usability, engagement, and effectiveness of the badges, and feedback mechanisms. This would better establish how such features contribute to long-term user behavioral change and cybersecurity awareness.

CHAPTER 5: EVALUATION

5.1. Usability Evaluation

Success in the web app for enhancing engagement and awareness of cyber security is dependent on its usability. Key usability metrics emphasized include learnability, efficiency, memorability, and satisfaction, to ensure ease in the usability of the app. The cognitive load of the interface is minimized to allow users to effect secure behaviors without much effort. New users will intuitively navigate the app and access the training modules with no difficulty in tracking their progress. In real-world practice, end-users interact with the web application through game-like cybersecurity training modules. The moment a persona logs in, they are shown a clear and clean dashboard emphasizing the availability of training modules and their progress throughout. The design of the training module overcomes many traditional challenges in cybersecurity training through gamification, such as disengagement caused by static content or a lack of real-time feedback: immediate feedback after quizzes, rewards with badges are just a couple of ways users remain engaged, motivated, and promote continuous participation. Expected outcomes entail better user comprehension and awareness of cybersecurity risks, including the ability to create better security habits. Customized feedback allows users to progress at their speed, therefore improving the retention of cybersecurity knowledge and reduction in riskier behaviors such as weak password usage or falling for phishing attacks.

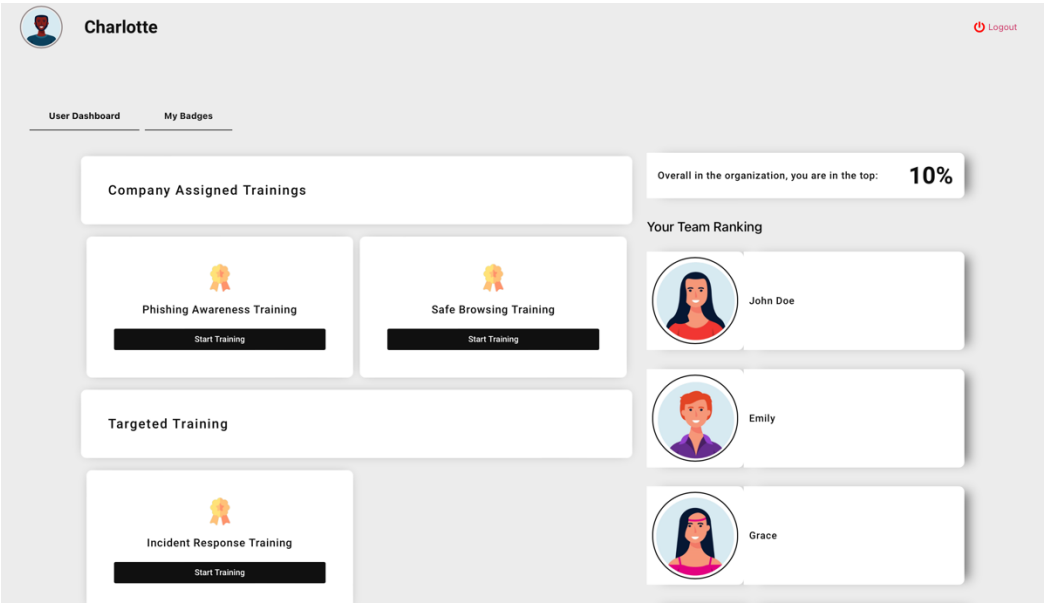

Figure 23: *Clear and Simple Navigation in the User Dashboard*

The dashboard will look and feel like from a user perspective, with clear navigation options such as "Company Assigned Training" and "Your Progress." Thus, a lack of unnecessary sophistication in layout saves the cognitive load of users, hence making them more capable of focusing on the content. This application makes certain that users can orient themselves easily in its ability to function and focus on accomplishing cybersecurity tasks with a clean, uncluttered interface, as shown in Figure 23.

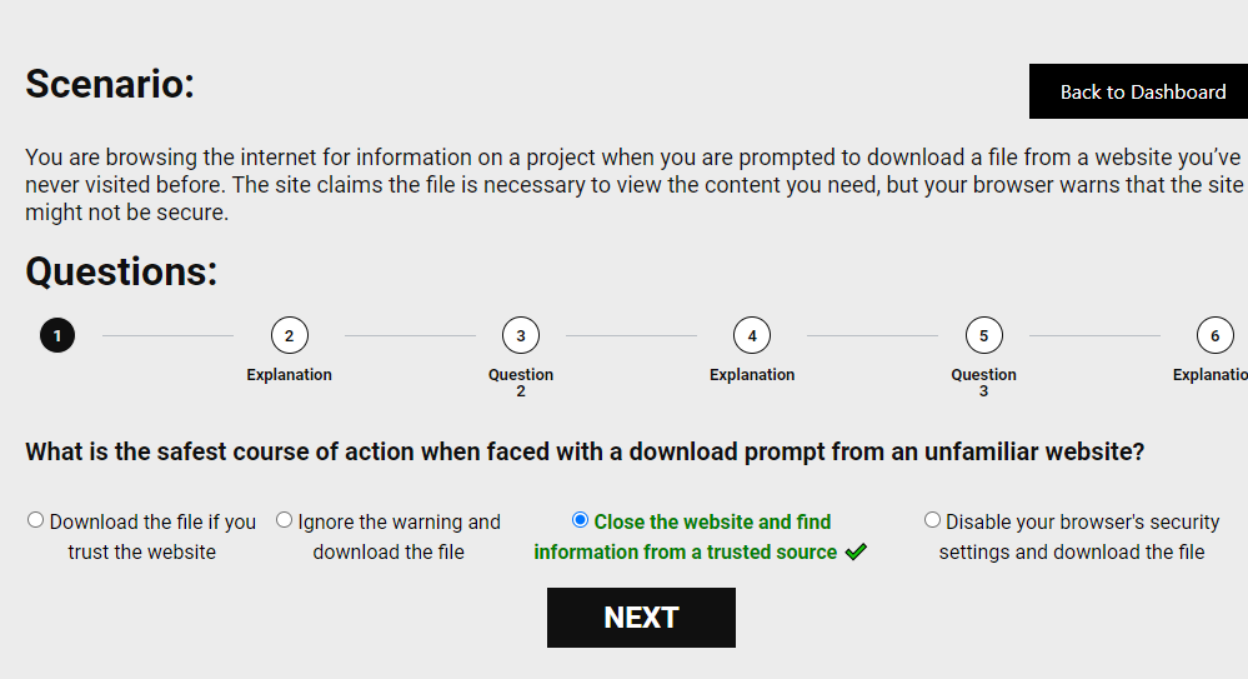

Figure 24: *Streamlined Interface for Efficient Task Completion in the Training Module*

Efficiency concerns the amount of time it takes for users to perform a certain task once they have learned to navigate the basic functionality of the app. An effective structure of the dashboard with links directing users to key features, as Figure 24 shows, will assist users in completing tasks with minimum navigation and clicks**.**

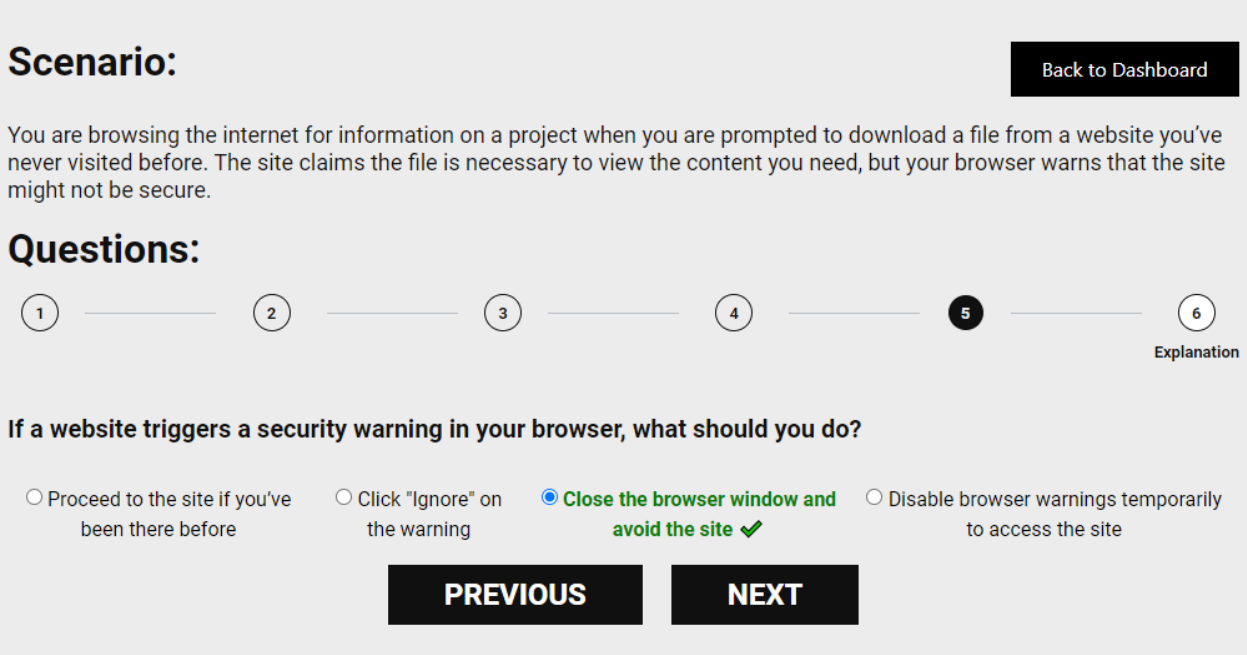

Figure 25: *Assisting users in completing Tasks*

Figure 25 depicts an interface that is clear and straightforward to the user for gaining access to and completing learning modules with as few steps as possible. Efficiency is enhanced further through real-time feedback and gamification elements that keep users interested without discouraging them from completing their tasks on time. Thoms et al. (2021) identify that enhancing efficiency in educational platforms increases users' feelings about interactions and increases the likelihood they will continue to longitudinally engage in training. Memorability is how easily users of the app, who have not used it for some time, can regain their proficiency. As indicated in Figure 26, the fact that menu bars and navigation buttons are designed to be consistent will make it easier for users to remember how to navigate between modules and features.

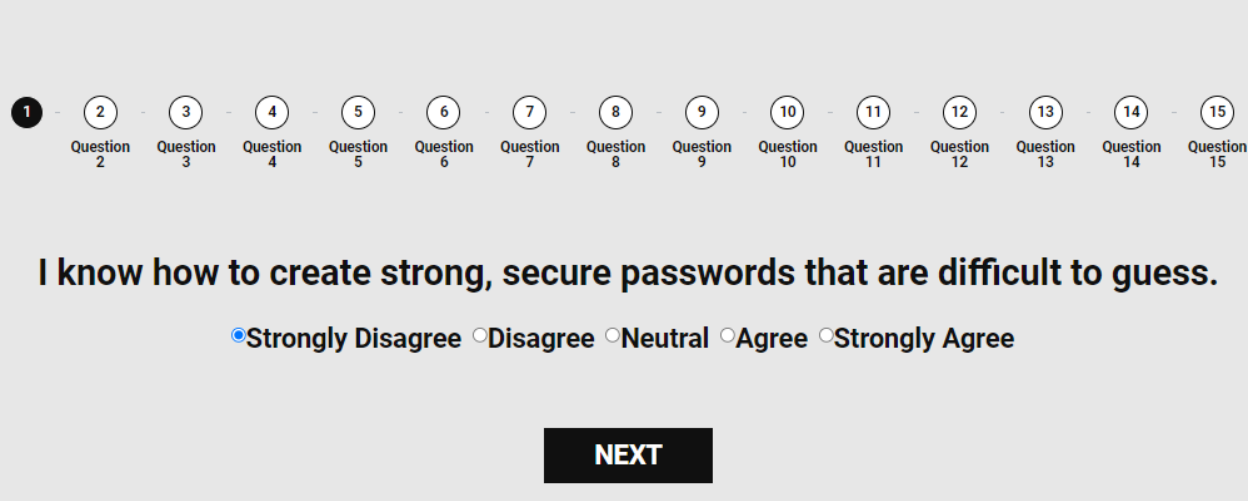

***Figure 26**: Consistent Layout and Design for Improved Memorability*

Gamification constituent features of the app, such as badges and leaderboard visibility, contribute a great deal toward user satisfaction since it turns what could otherwise be a dry learning process into an engaging one that is rewarding. This view is supported in Hamari et al. (2019), where gamification techniques, through progress tracking and rewards, create a sense of achievement that enhances users' motivation for further engagement with the training.

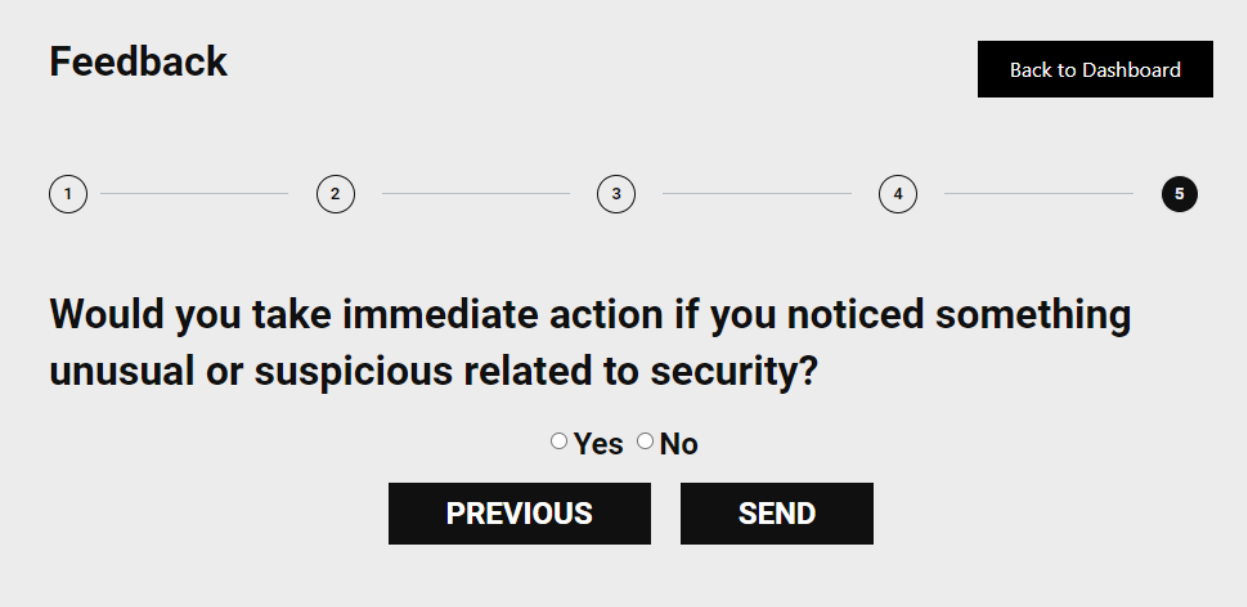

***Figure 27**: Immediate Feedback Following Quiz Completion for Enhanced User Satisfaction*

Smooth integration of real-time feedback in the application further enhances the user experience; making them feel guided and taken care of throughout the training. Immediate feedback, shown in Figure 27, helps users gauge their cybersecurity awareness after every training.

5.2. Engagement Evaluation

Engagement is one of the most vital aspects of any educational tool, especially when there is special training in cybersecurity, in which the users have to be constantly motivated toward completion for practical implementation. The web application harvests various engagement features, such as virtual activities, quizzes, and gamification attributes that will allow users to take active participation for increased completed training. The functions allow users to practice cybersecurity scenarios from a safe, controlled space.

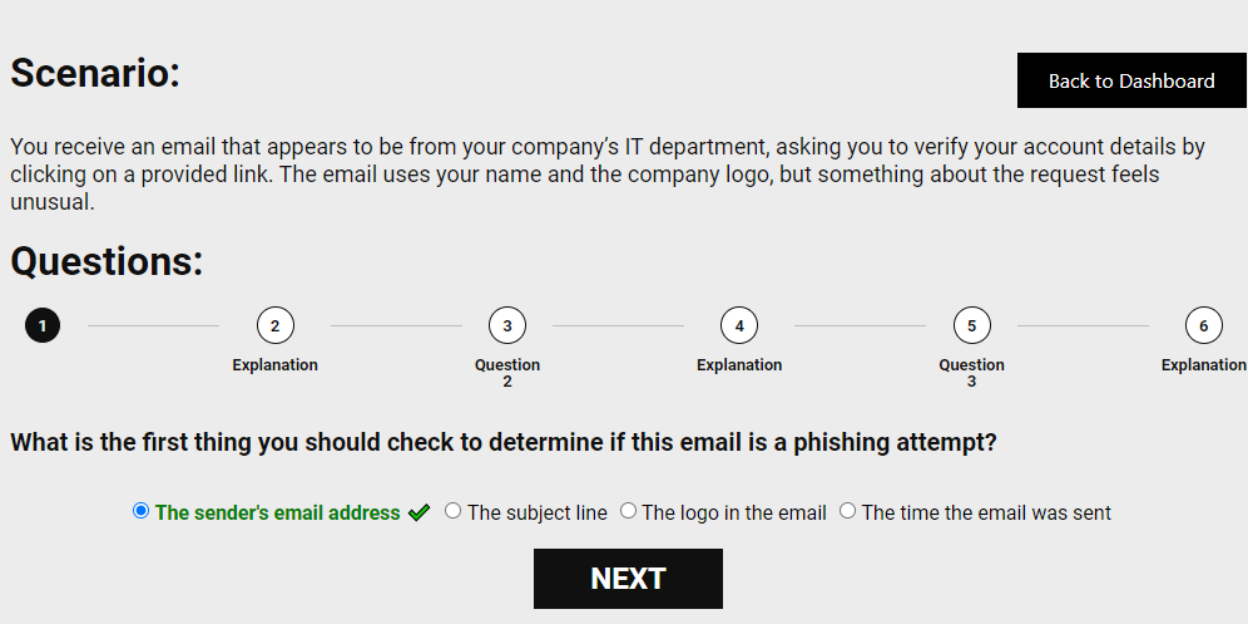

Figure 28: *Engaging Users with a Phishing Simulation in the Training Module*

Figure 28 shows an interactive phishing simulation in which users are asked to identify signs of a phishing email. Hamari et al. (2024) further explain that simulations make the process of learning active, not passive; thus, enable active interaction instead of reading or watching passively. This real-time feedback, according to Saxena et al. (2021), is the cornerstone to maintaining the user's

level of engagement since it ets the user feel that he or she has completed a task and the result thereof, including his or her mistakes being corrected.

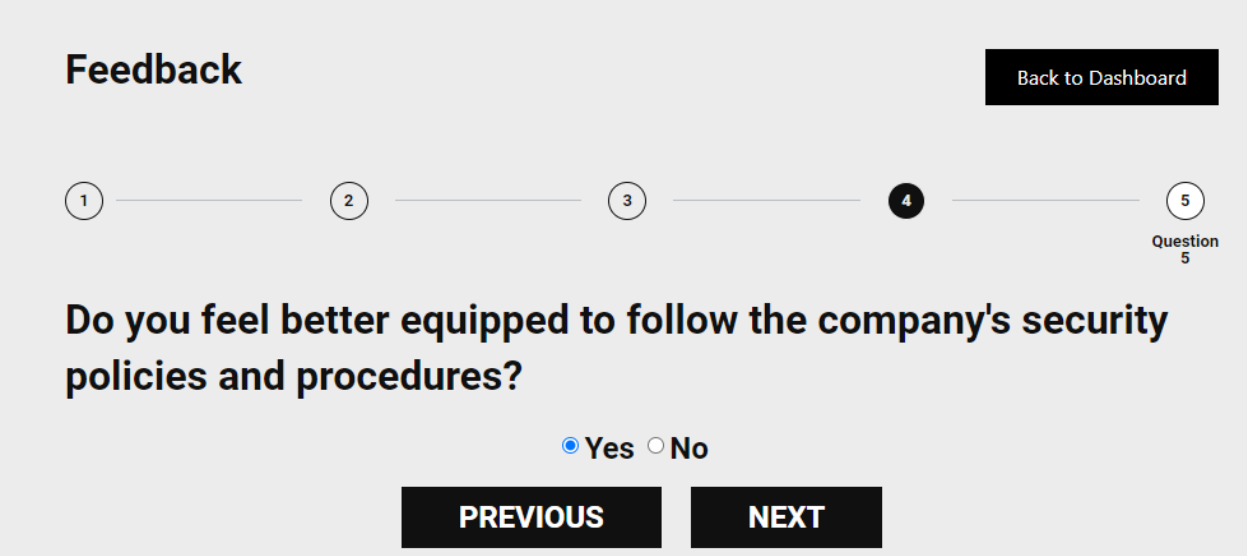

Figure 29: *Immediate Feedback After a Quiz to Enhance User Engagement*

Figure 29 illustrates the immediate feedback provided to users after completing a quiz, a key feature designed to enhance engagement and reinforce learning outcomes by showing correct or needed improvements directly. Quizzes will also offer a source of accomplishment since users can observe their progress over time. Other Gamification Elements Other elements that are integrated into the gamification in the web app, apart from simulations and quizzes, include badges and progress indicators for enhancing user engagement further.

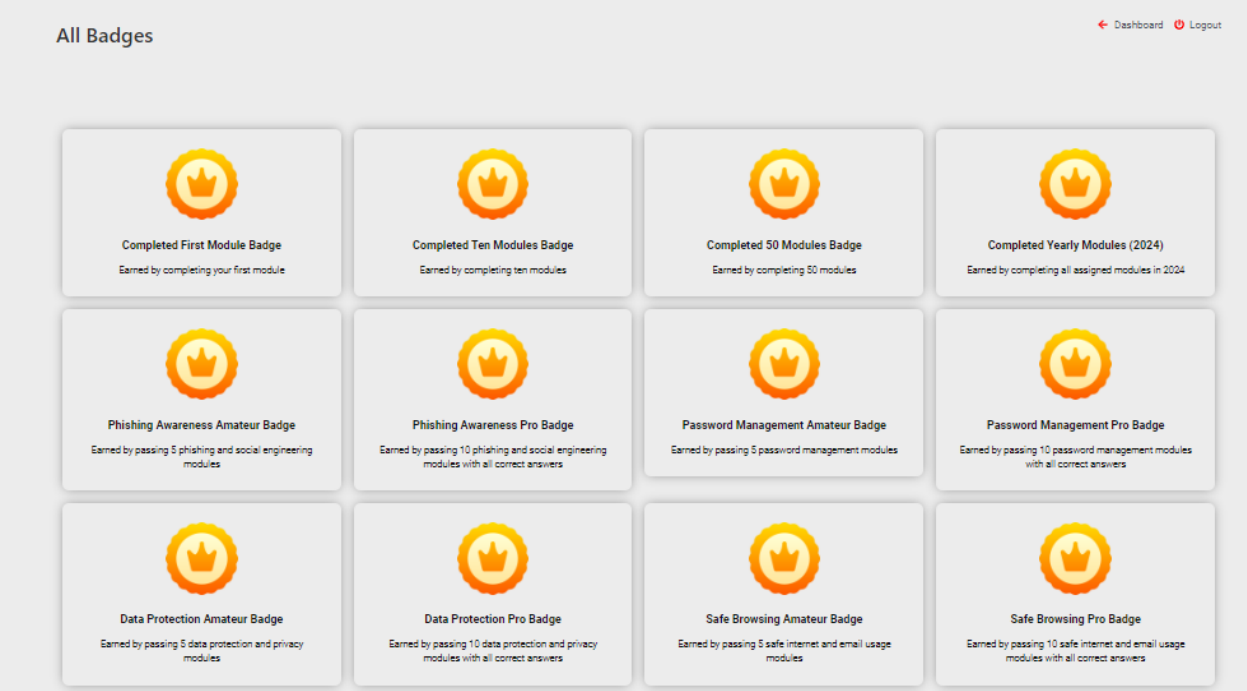

Figure 30: *Gamification Through Badges to Motivate and Engage Users*

Figure 30 highlights the use of gamification in the form of badges, which are awarded to users to motivate and maintain engagement by recognizing their achievements and progress in cybersecurity practices. Giving badges and leader boards gives the idea a competitive edge and works very effectively, notes Thoms et al. (2021) in their work. As a result, the web app offers utilitarian incentives that make users more active and engaged in training more modules. Its evaluation criteria will consist of the degree of participation witnessed among the users as well as the conversion rates as the users complete tasks in their usual routines as well as their behavioral changes during the use of the specific technology.

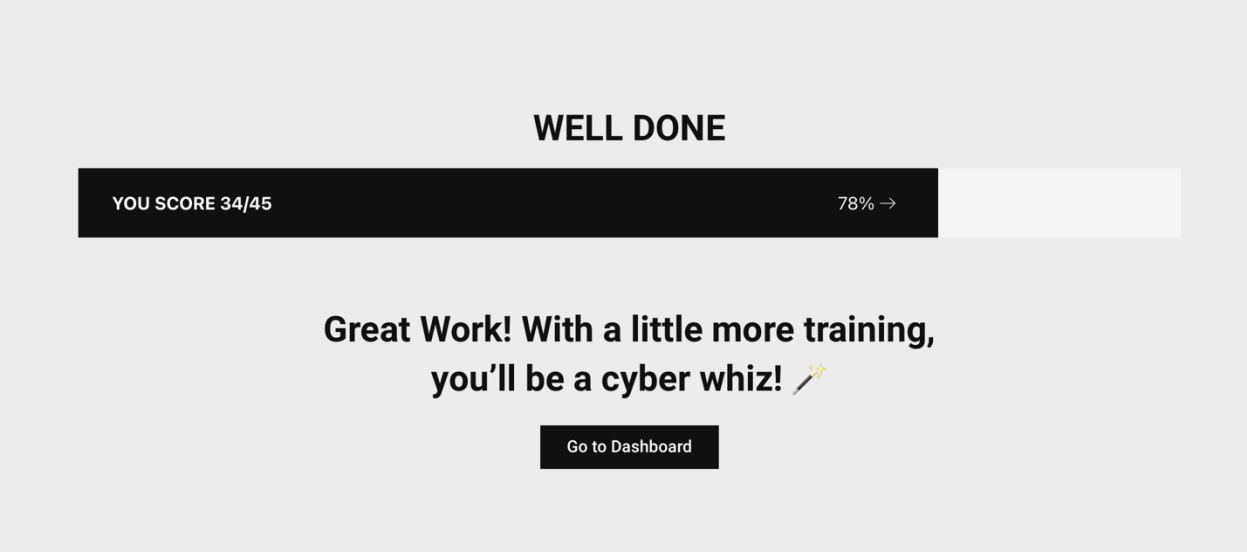

***Figure 31**: Baseline Assessment Completion*

Figure 31 displays a baseline score from completing the onboarding assessment, showing a user's score of 34/45 or 78%, accompanied by a motivational message that encourages further learning to achieve mastery in cybersecurity.

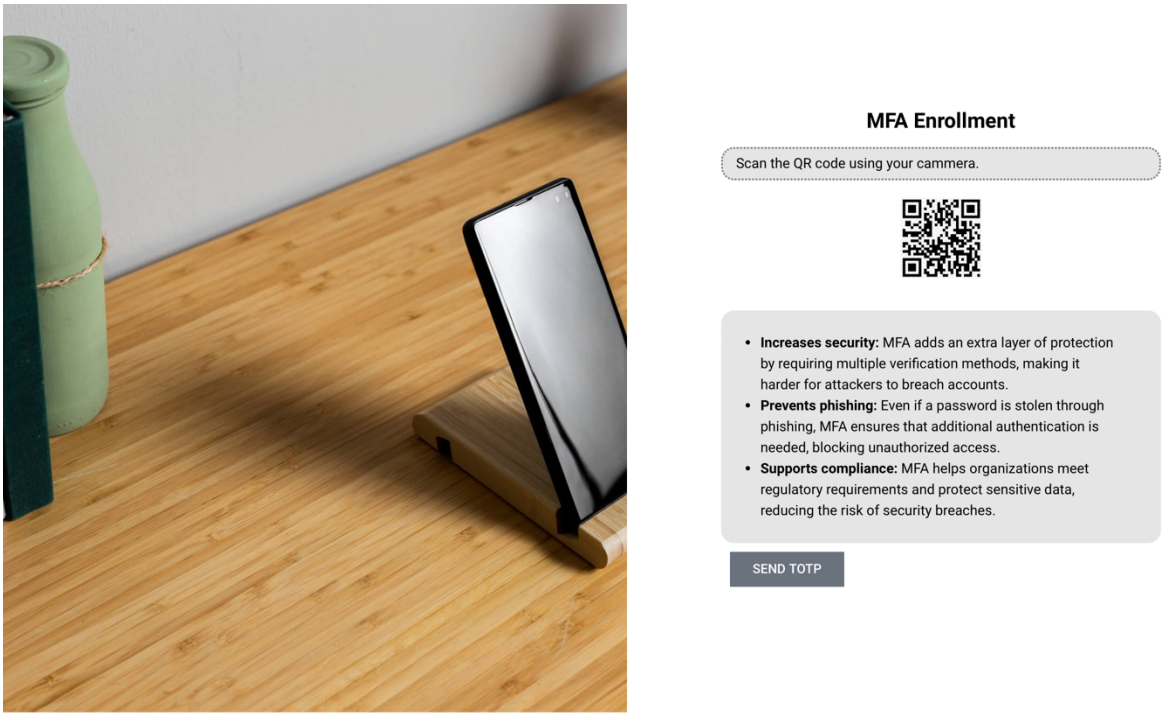

***Figure 32:** MFA Enrollment Interface*

Figure 32 shows the MFA enrollment screen on a mobile device, advertising enhanced security by scanning a quick response - QR code for setup. The screen interface will also identify that MFA increases security, prevents phishing, and complies with policies, all to keep user accounts safe

from unauthorized access. According to Mayer and Moreno (2017), providing visual cues like full display of number of questions enhances engagement by offering users a clear goal to work towards, which increases their commitment to completing the training. These features not only make the learning process more enjoyable but also ensure that users remain motivated and committed to completing the training, thereby enhancing overall cybersecurity awareness.

5.3. Behavior Change Evaluation

Behavior change is essential for improving cybersecurity hygiene, as human error remains a significant vulnerability in organizations. In this section, we evaluate how the web app leverages behavior reinforcement mechanisms such as progress indicators and badges to promote long-term user engagement and improve security practices. The web app uses progress indicators to provide users with continuous feedback on their advancement through various training modules. This is supported by research from Sweller et al. (2019), which highlights the positive impact of consistent feedback on user engagement and task completion.

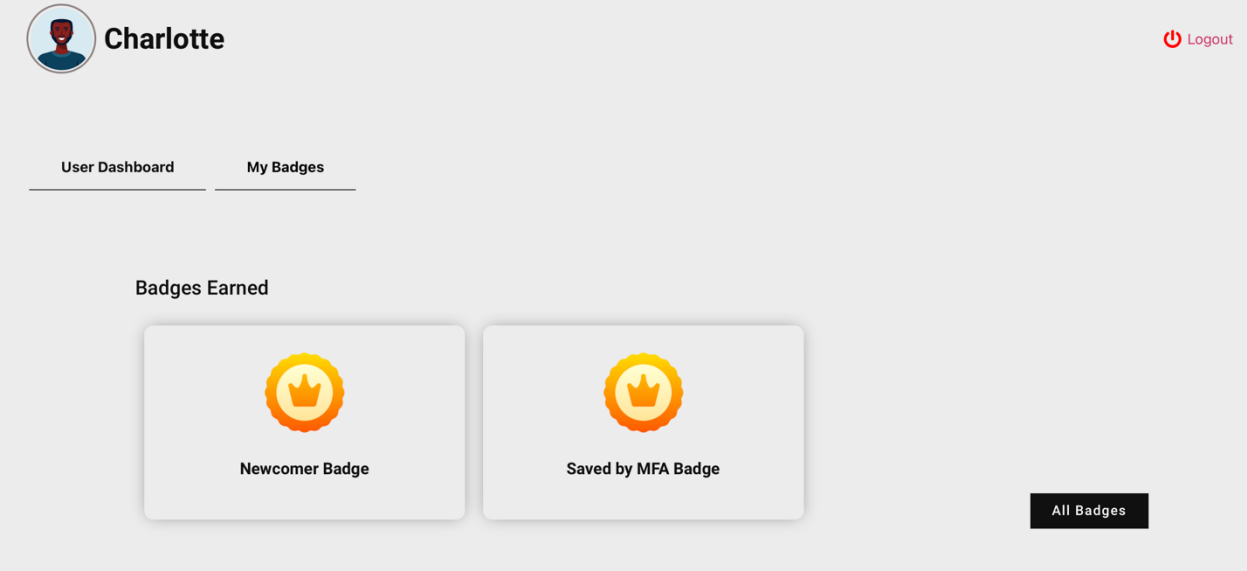

***Figure 33**: User Profile and Achievement Display in Cybersecurity Training Platform*

In Figure 33 this is the profile of 'Charlotte', as visible on this cybersecurity training platform. The section entitled 'Badges Earned' is highlighted with badges entitled 'Newcomer Badge' and 'Saved by MFA Badge'. These badges are varied motivators to reward the user for their progress and achievement in respect to certain objectives of the training program, encouraging them to ensure continued engagement and learning of cybersecurity practices. Badges, another critical component

of the app, serve as a reward system that recognizes users for completing specific actions, such as finishing training modules or setting up multi-factor authentication (MFA).

Moreover, gamification the incorporation of game-like features into non-gaming contexts has been widely adopted in educational and training programs to increase user engagement and participation. Research by Thoms et al. (2021) suggests that gamification not only boosts short-term engagement but also leads to long-term behavior change, as users internalize the lessons they learn and continue to apply them outside of the app.

5.4. Learning Section

The web app development was useful to gain experience in applying a UX-centered approach in cybersecurity training. Some of the important experience implications include the need to present the contents in a simple form, the need to provide feedback that is almost immediate to enhance learning, and the use of the game features to enhance the users' interest. These suggestions can be implemented in the subsequent version of the app where more efforts will be put to deal with the shortcomings of the current prototype.

Chapter 5 was concluded by an in-depth analysis of the usability, engagement, and change in behavior brought along by the web application. Although the results were promising, it was apparent that more refinement had to be carried out to retain the best interaction with users for long-lasting behavior changes. This chapter will now address the limitations of the current prototype, discussing the constraints that occurred during development and evaluation. The limitations that will be discussed will eventually provide insight for future iteration and improvement.

CHAPTER 6: LIMITATIONS

While solid UX-driven design informed its development, underpinned by sound theories of behavioral change, there are a number of limitations that have to be identified. One major limitation of this paper is that it has been recognized concerning various stages of the development and testing without real-world users. This is a prototype app developed based on theoretical perspectives rather than direct user feedback in the form of prototype testing. While this in no way merely underscores the validity of the project, it does point to the fact that for any further refinements in design and functionality, real users need to be involved in the future. Real user feedback is lacking in large parts, regarding how well the app performs in practical environments. A test plan of what will be clearly defined for the future includes key metrics such as user engagement, completion rates of behaviors, and actual measured change in behavior.

These will be beneficial in understanding how well the application has been able to induce long-term behavioral changes in safe cybersecurity practices. Additionally, a very good enhancement in the future versions is assuring that feedback is given only after the completion of the training modules and not right after the selection of every option. This makes critical thinking and engagement more engaging before the feedback is delivered. This is something that should be revised for future testing, as with the current prototype, users get an immediate answer no matter which option they choose. While the Cognitive Load Theory has been supported by some research, such as Sweller et al. (2019), and the gamification strategies were placed upon a rather heavy foundation of theory, for example, Hamari et al. (2019), an empirical test is needed to confirm in practice the real life effect of such theories. In this regard, iterative user testing will be fundamental in locating pain points and further enhancing general user satisfaction. Considering the current prototype, it stands to demonstrate the operationalization of UX-centered cybersecurity design principles; however, further refinement with real-world data is critical to its long-term validation for effectiveness. The limitation of the app at present is, therefore, one of not being tested in the real world, but this need not undermine its credibility or academic contribution in any way. The next steps involve obtaining user feedback, further refinement of the system of delivery of feedback, and evaluation of behavior change using measures of user performance and user engagement metrics.

Chapter 6 described some limitations of the current prototype, which does not include user testing in the real world and iterative feedback. Such limitations do not make any question about the

credibility or academic merit of this project, provided it can reveal how the operationalization of UX-centered design principles into cybersecurity training is based upon well-identified theoretical frameworks. Chapter 7 now proceeds with the recommendations of the future on how this prototype could be further refined through real-world testing, iterative improvement, and long-term studies. In this way, it furthers the validation of the web application as an effective tool in cybersecurity awareness training.

CHAPTER 7: FUTURE RECOMMENDATIONS

7.1. Primary Research & User Feedback

Currently, the web application is developed about the theoretical application of UX-centered principles. Further research should focus on real-world user testing concerning the existence of a prototype to confirm or alter the design concerning actual preferences and needs of active users. User testing would indicate substantially important insights into how well and in what ways different people make sense of and can use the features of an application; therefore, a much deeper analysis would be possible concerning whether the design corresponds to the needs of the users. Feedback about interface intuitiveness, user engagement with the training modules, and whether the application effectively simplifies complex cybersecurity concepts could be solicited through usability testing, surveys, and focus groups.

Real-world testing would also become necessary to reveal any points of friction or confusion for the users. For example, testing may show where the user has an easy time logging in or if the gamification elements encourage them to go through the training. Moreover, user performance data could be represented by the time taken to complete modules or the percentage of their correct answers in quizzes, providing measurable outcomes related to the app's effectiveness in improving cybersecurity awareness and behavior. This would transform the app from a theoretical artefact into a validated tool that enhances organizational security training.

7.2. Iterative Development

Building upon that knowledge acquired through feedback from the users, these features should be iteratively refined and made even more usable in the web application by further development. This development could also enable adaptive learning paths where the application dynamically adjusts the trainings to fit the performance and needs of a user. For example, those users who show a better level of understanding of certain cybersecurity concepts may immediately proceed to higher modules, while other users who have difficulties with them are given further support or alternative explanations.

Future development could be made by devising more personalized feedback mechanisms. While the app, as of now, does provide real-time feedback right after quizzes, in future versions there could be more detailed insights including further learning recommendations based on user performance. Also, reminders and notifications regarding pending work or upcoming deadlines improve the user's involvement in encouraging persistent participation in the app. These features

would be even more fine-tuned with the integration of artificial intelligence or machine learning, wherein the app learns from user behavior and provides more personalized content and feedback over time.

7.3. Longitudinal Studies

Apart from this, short-term usability testing, the effectiveness with which the web app promotes continued behavioral changes for long periods should be determined using longitudinal studies. The need is there for extended measured retention of the knowledge and skills the app imparts on the users for its true impact to manifest since cybersecurity awareness training is behavior that should be inculcated within an individual to reduce human errors leading to security breaches.

This could even be a longitudinal study in which the users of the application are followed for long periods of several months or years-and the permanency of improvement in practices related to password management, phishing awareness, and adherence to security protocols is examined. Periodic surveys and performance assessments would be undertaken to analyze changes in user behavior and to see whether gamification elements and real-time feedback cause long-lasting motivational results. The longitudinal research would further allow the analysis of how well the app can adapt to the changing conditions within organizations.

7.4. Key Challenges

Throughout the course of this project, a few key, major issues evolved that need to be taken into consideration in further development. The main challenges facing the system are related to real-world user testing. Since there is no direct input from the users of this system, its current design and functionality are based on mere theory. This does leave holes in the potential usability and effectiveness of the system. Because user feedback is absent, refinement of features for better engagement and learning outcomes cannot be attained. Other areas of challenge involve the back-end functionality and scalability of the application. The application is still at a prototype stage and has not implemented some key backend functionalities such as authentication or RBAC, important in providing secure and scalable deployment in an organizational environment. For example, scalability in respect of handling a large number of users and adaptability to the requirements of various organizations needs to be tested and optimized in future versions.

7.5.Limitations

The focus for future work should be the integration of user feedback into the development process, enhancement of the functionality in the backend, and iteration of the UX design based on real-world data. Some concrete next steps could be:

- **User Feedback Incorporation:** Perform extensive usability testing with actual users; obtain detailed qualitative feedback about interface design, navigation, and user engagement; implement improvements based on data collected.
- **Improved Backend Development:** Integrate proper authentication, such as multi-factor authentication and RBAC for different user roles, to make the application secure.
- UX Design Iteration Refines the UX design to integrate real-world insights in enhancing navigation, feedback timing, and gamification elements.
- **Improving Scalability:** The performance of the app should be tested in highly populated environments to ensure it can scale up, maintaining smooth functionality.

CONCLUSION

This research has shown that the UX-centered design can improve the awareness of cybersecurity through an actual web application. The web app references basic concepts of UX and links them with the practical implementation in the form of long-term behavioral change. The future studies should also involve improvement of the app and its modification based on the users' feedback and actual trials and errors to prove the app's efficiency. Further, the improved backend and the augmentations of the security measures will be crucial for further scaling up of the app within the organizational environment. This research has shown one way of applying the UX-centered framework for cybersecurity awareness training through the web app. The fundamental concepts of UX are applied in the application, namely, interaction, simplification of information and its feedback as well as behavior enhancement, this illustrates how theories are practically applied in a tool that fosters improved cybersecurity practices among users. This research has conclusively shown that usability is a crucial aspect of the security training program design, enhancing user participation, comprehension, and long-term retention of critical information.

The web application serves as an artifact that bridges the gap between theory and practice, operationalizing established theories such as Cognitive Load Theory and Behavioral Change Theories. Although it hasn't been tested on real users, the design is based on best practices and provides substantial academic value. By using gamification techniques such as badges and progress indicators, along with real-time feedback, the app encourages and sustains user interest in security-related behaviors, surpassing traditional training methods. Additionally, the web application's flexibility and scalability allow it to adapt to various organizational contexts, providing a customizable tool for addressing specific security risks and enhancing Cybersecurity Posture. However, as the current version is a theoretical implementation, further research should include iterative development to improve integration of user feedback and adaptive learning.

Thus, this work effectively demonstrates how UX-centered design can be applied to cybersecurity training, adding value to both academic research and practice by providing a framework for increasing user engagement, simplifying complex information, and promoting long-term behavioral change. Continued development and validation through real-world testing will ensure the app remains relevant and effective in addressing the evolving challenges in cybersecurity awareness training.

REFERENCES

Ajzen, I., 1991. The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50(2), pp.179-211. https://doi.org/10.1016/0749-5978(91)90020-T

Ala'a, M., Ramayah, T., & Al-Sharafi, M. A. (2024). Exploring the impact of cybersecurity on using electronic health records and their performance among healthcare professionals: A multi-analytical SEM-ANN approach. *Technology in Society*, 77, 102592.

Alibhai, M. (2021). Cybersecurity attacks on academic data and personal information and the mediating role of education and employment. *Journal of Computer and Communications*, 9(11), 77-90.

Alqahtani, H., Kavakli-Thorne, M., & Alrowaily, M. (2020). The impact of gamification factor in the acceptance of cybersecurity awareness augmented reality game (CybAR). In *HCI for Cybersecurity, Privacy and Trust: Second International Conference, HCI-CPT 2020, Copenhagen, Denmark, July 19–24, 2020, Proceedings 22* (pp. 16-31). Springer International Publishing.

Alquran, H. (2023). Towards sustainable e-learning platforms in the context of cybersecurity: A TAM-driven approach (Doctoral dissertation, Eastern Michigan University).

Al-Zahrani, M. (2020). Integrating IS success model with cybersecurity factors for e-government implementation in the Kingdom of Saudi Arabia. *International Journal of Electrical and Computer Engineering*, 10(5), 4937-4955.

Anderson, C.L. and Agarwal, R., 2010. Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. *MIS Quarterly*, 34(3), pp.613-643. https://doi.org/10.2307/25750694

Baker, M. B., Sihwail, R., & Mizher, M. (2023, October). Integrating cyber security factors with TAM framework for implementation in the Jordanian banks. In *AIP Conference Proceedings* (Vol. 2979, No. 1). AIP Publishing.

Bandura, A., 1986. *Social foundations of thought and action: A social cognitive theory*. Prentice-Hall.

Cheung, K. F., Bell, M. G., & Bhattacharjya, J. (2021). Cybersecurity in logistics and supply chain management: An overview and future research directions. *Transportation Research Part E: Logistics and Transportation Review*, 146, 102217.

Costley, J. and Lange, C. (2020). The effects of instructor control on social presence: Variations within online learning environments. *Journal of Educational Computing Research*, 58(4), pp.795-813. https://doi.org/10.1177/0735633119886067

Costley, J. and Lange, C., 2017. The effects of instructor control on critical thinking and social presence: Variations within three online asynchronous learning environments. *Journal of Educational Computing Research*, 55(8), pp.1013-1034. https://doi.org/10.1177/0735633116688317

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review*, 4(10).

Da Veiga, A. (2016, July). A cybersecurity culture research philosophy and approach to develop a valid and reliable measuring instrument. In *2016 SAI Computing Conference (SAI)* (pp. 1006-1015). IEEE.

Dasgupta, D., Akhtar, Z., & Sen, S. (2022). Machine learning in cybersecurity: A comprehensive survey. *The Journal of Defense Modeling and Simulation*, 19(1), 57-106.

Dash, B., & Ansari, M. F. (2022). An effective cybersecurity awareness training model: First defense of an organizational security strategy.

De Kimpe, L., Walrave, M., Verdegem, P., & Ponnet, K. (2022). What we think we know about cybersecurity: An investigation of the relationship between perceived knowledge, internet trust, and protection motivation in a cybercrime context. *Behaviour & Information Technology*, 41(8), 1796-1808.

Deterding, S., Dixon, D., Khaled, R. and Nacke, L., 2011. From game design elements to gamefulness: Defining "gamification". In *Proceedings of the 15th International Academic MindTrek Conference*, pp.9-15. https://doi.org/10.1145/2181037.2181040

Dinev, T. and Hart, P., 2006. An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, 17(1), pp.61-80. https://doi.org/10.1287/isre.1060.0080

Dixit, P., & Silakari, S. (2021). Deep learning algorithms for cybersecurity applications: A technological and status review. *Computer Science Review*, 39, 100317.

Dodge, C. E., Fisk, N., Burruss, G. W., Moule Jr, R. K., & Jaynes, C. M. (2023). What motivates users to adopt cybersecurity practices? A survey experiment assessing protection motivation theory. *Criminology & Public Policy*, 22(4), 849-868.

Dombrowski, L., Harmon, E. and Fox, S. (2020). Digital Security as Care: Evaluating Data-Driven Health Technologies in Social Care Work. *Proceedings of the ACM on Human-Computer Interaction*, 4(CSCW), pp.1-29. https://doi.org/10.1145/3432925

Doroftei, D., De Cubber, G., Wagemans, R., Matos, A., Silva, E., Lobo, V., & Serrano, D. (2017). User-centered design. *Search and Rescue Robotics from Theory to Practice*, 19-36.

Ebot, A. (2024). Technology Acceptance Model for Adopting Cybersecurity Technology in Small and Medium Business/Enterprise: A Generic Qualitative Study (Doctoral dissertation, Capella University).

Endsley, M.R., 1995. Toward a theory of situation awareness in dynamic systems. *Human Factors*, 37(1), pp.32-64. https://doi.org/10.1518/001872095779049543

Endsley, M.R., 1995. Toward a theory of situation awareness in dynamic systems. *Human Factors*, 37(1), pp.32-64. https://doi.org/10.1518/001872095779049543

Fogg, B.J., 2009. A behavior model for persuasive design. In *Proceedings of the 4th International Conference on Persuasive Technology*, pp.1-7. https://doi.org/10.1145/1541948.1541999

Furnell, S. and Thomson, K., 2009. From culture to disobedience: Recognizing the varying user acceptance of IT security. *Computer Fraud & Security*, 2009(2), pp.5-10. https://doi.org/10.1016/S1361-3723(09)70017-3.

Hadlington, L., 2017. Human factors in cybersecurity: Examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky online behaviours. *Heliyon*, 3(7), p.e00346. https://doi.org/10.1016/j.heliyon.2017.e00346

Hamari, J., Koivisto, J. and Sarsa, H. (2019). Does gamification work? A literature review of empirical studies on gamification. *Proceedings of the 47th Hawaii International Conference on System Sciences*, pp.3025-3034. https://doi.org/10.1109/HICSS.2014.377

Herley, C., 2016. The plight of the unwitting user. *Communications of the ACM*, 55(6), pp.22-24. https://doi.org/10.1145/2181037.2181040

Kahneman, D., 2011. *Thinking, fast and slow*. Farrar, Straus and Giroux.

Koivisto, J. and Hamari, J. (2019). The rise of motivational information systems: A review of gamification research. *International Journal of Information Management*, 45, pp.191-210. https://doi.org/10.1016/j.ijinfomgt.2018.10.013

Krug, S., 2014. *Don't Make Me Think, Revisited: A Common Sense Approach to Web Usability*. New Riders.

Mayer, R.E. and Moreno, R. (2017). Nine ways to reduce cognitive load in multimedia learning. *Educational Psychologist*, 38(1), pp.43-52. https://doi.org/10.1207/S15326985EP3801_6

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M. and Pattinson, M., 2017. Individual differences and information security awareness. *Computers & Security*, 70, pp.476-489. https://doi.org/10.1016/j.cose.2017.08.003

Miller, G.A., 1956. The magical number seven, plus or minus two: Some limits on our capacity for processing information. *Psychological Review*, 63(2), pp.81-97. https://doi.org/10.1037/h0043158

Muntean, C.I. (2018). Raising engagement in e-learning through gamification. *Proceedings of the 6th International Conference on Virtual Learning*. Available at: https://www.icvl.eu (Accessed: 10 March 2024).

Nielsen, J., 1993. *Usability Engineering*. Academic Press.

Nielsen, J., 1994. *Usability engineering*. Morgan Kaufmann.

Norman, D.A., 1988. *The Psychology of Everyday Things*. Basic Books.

Norman, D.A., 2013. *The Design of Everyday Things* (Revised ed.). Basic Books.

Paas, F. and van Gog, T., 2019. Cognitive load theory: Methods to manage working memory load in the learning process. *Current Opinion in Behavioral Sciences*, 29, pp.86-90. https://doi.org/10.1016/j.cobeha.2019.04.001

Pino, A., Marrone, M. and Di Bitonto, P. (2020). How digital gamification can improve learning: Development and initial validation of a self-report questionnaire on gamified e-learning. *Computers & Education*, 144, 103697. https://doi.org/10.1016/j.compedu.2019.103697

Prinsloo, P. and Slade, S., 2017. Big data, higher education and learning analytics: Beyond justice, towards an ethics of care. *Assessment & Evaluation in Higher Education*, 42(6), pp.957-968. https://doi.org/10.1080/02602938.2016.1164828

Ryan, R.M. and Deci, E.L., 2000. Self-Determination Theory and the facilitation of intrinsic motivation, social development, and well-being. *American Psychologist*, 55(1), pp.68-78. https://doi.org/10.1037/0003-066X.55.1.68

Sailer, M., Hense, J., Mayr, S. and Mandl, H., 2017. How gamification motivates: An experimental study of the effects of specific game design elements on psychological need satisfaction. *Computers in Human Behavior*, 69, pp.371-380. https://doi.org/10.1016/j.chb.2016.12.033

Sasse, M.A., Brostoff, S. and Weirich, D., 2001. Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security. *BT Technology Journal*, 19(3), pp.122-131. https://doi.org/10.1023/A:1011902718709

Saxena, K., Kumar, A. and Goyal, A. (2020). Impact of real-time feedback in e-learning: A study of its effectiveness in promoting better learning outcomes. *Journal of Educational Technology Systems*, 48(3), pp.463-482. https://doi.org/10.1177/0047239519886067

Shneiderman, B., 1992. *Designing the User Interface: Strategies for Effective Human-Computer Interaction*. Addison-Wesley.

Skinner, B.F., 1953. *Science and Human Behavior*. Simon and Schuster.

Sweller, J., 1988. Cognitive load during problem-solving: Effects on learning. *Cognitive Science*, 12(2), pp.257-285. https://doi.org/10.1207/s15516709cog1202_4

Sweller, J., Ayres, P. and Kalyuga, S. (2019). *Cognitive load theory in instructional design*. Springer. https://doi.org/10.1007/978-1-4419-8126-4

Thoms, B., Garrett, N. and Ryan, C. (2018). The effectiveness of gamified training on promoting good cybersecurity behaviors: A longitudinal study. *Computers & Security*, 77, pp.253-262. https://doi.org/10.1016/j.cose.2018.03.011

Thoms, B., Garrett, N. and Ryan, C. (2021). Gamification and real-time feedback in cybersecurity training: Assessing engagement and performance. *Computers & Security*, 92, 101743. https://doi.org/10.1016/j.cose.2020.

Verizon, 2021. *2021 Data Breach Investigations Report*. Available at: https://www.verizon.com/business/resources/reports/dbir/.

Vishwanath, A., Herath, T., Chen, R., Wang, J. and Rao, H.R., 2016. Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems*, 51(3), pp.576-586. https://doi.org/10.1016/j.dss.2011.03.002

Werbach, K. and Hunter, D., 2012. *For the win: How game thinking can revolutionize your business*. Wharton Digital Press.

Wickens, C.D., Hollands, J.G., Banbury, S. and Parasuraman, R. (2019). *Engineering psychology and human performance*. Routledge. https://doi.org/10.4324/9781315227802

Zichermann, G. and Cunningham, C., 2011. *Gamification by design: Implementing game mechanics in web and mobile apps*. O'Reilly Media, Inc.

Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). *Cyber Security Awareness Campaigns: Why do they fail to change behaviour?* (arXiv:1901.02672). arXiv. http://arxiv.org/abs/1901.02672

Barendse, S. W. (2023). *Exploring Gamification and Cybersecurity: How Could Gamification Increase the Cybersecurity Awareness*. http://arno.uvt.nl/show.cgi?fid=161617

Billman, C. (2024). *Navigating Trust: The Impact of UI Usability on Perceived Security*. https://www.diva-portal.org/smash/record.jsf?pid=diva2:1866385

Bitrián, P., Buil, I., Catalán, S., & Merli, D. (2024). Gamification in workforce training: Improving employees' self-efficacy and information security and data protection behaviours. *Journal of Business Research*, *179*, 114685.

Faith, B. F., Long, Z. A., & Hamid, S. (2024). Promoting cybersecurity knowledge via gamification: An innovative intervention design. *2024 Third International Conference on Distributed Computing and High Performance Computing (DCHPC)*, 1–8. https://ieeexplore.ieee.org/abstract/document/10454080/

Gratian, M., Bandi, S., Cukier, M., Dykstra, J., & Ginther, A. (2018). Correlating human traits and cyber security behavior intentions. *Computers & Security*, *73*, 345–358.

Gunduz, M. Z., & Das, R. (2020). Cyber-security on smart grid: Threats and potential solutions. *Computer Networks*, *169*, 107094.

Hadlington, L. (2018). The "human factor" in cybersecurity: Exploring the accidental insider. In *Psychological and behavioral examinations in cyber security* (pp. 46–63). IGI Global. https://www.igi-global.com/chapter/the-human-factor-in-cybersecurity/199881

Homoliak, I., Toffalini, F., Guarnizo, J., Elovici, Y., & Ochoa, M. (2020). Insight Into Insiders and IT: A Survey of Insider Threat Taxonomies, Analysis, Modeling, and Countermeasures. *ACM Computing Surveys*, *52*(2), 1–40. https://doi.org/10.1145/3303771

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, *45*, 13–24.

Lindgren, N. (2020). *How can gamification enable behavior change related to information security: A literature review*. https://www.diva-portal.org/smash/record.jsf?pid=diva2:1471260

Liu, L., De Vel, O., Han, Q.-L., Zhang, J., & Xiang, Y. (2018). Detecting and preventing cyber insider threats: A survey. *IEEE Communications Surveys & Tutorials*, *20*(2), 1397–1417.

Malinina, P. (2023). *How Generative AI will change work in IT in the near future*. https://www.theseus.fi/handle/10024/810563

Martin, S. (2018). Measuring cognitive load and cognition: Metrics for technology-enhanced learning. In *Technology-Enhanced and Collaborative Learning* (pp. 77–106). Routledge. https://www.taylorfrancis.com/chapters/edit/10.4324/9781315270111-5/measuring-cognitive-load-cognition-metrics-technology-enhanced-learning-stewart-martin

Nguyen, D., & Ng, D. (2022). Teacher collaboration for change: Sharing, improving, and spreading. In *Leadership for Professional Learning* (pp. 178–191). Routledge. https://www.taylorfrancis.com/chapters/edit/10.4324/9781003357384-12/teacher-collaboration-change-sharing-improving-spreading-dong-nguyen-david-ng

Sharma, S. P. (2024). Impact of HR Analytics for Talent Acquisition in Identifying Quality Resources. *International Journal of Innovative Research in Engineering & Management*, *11*(1), 43–50.

Silic, M., & Lowry, P. B. (2020). Using Design-Science Based Gamification to Improve Organizational Security Training and Compliance. *Journal of Management Information Systems*, *37*(1), 129–161. https://doi.org/10.1080/07421222.2019.1705512

Tatum, D. (2023). *Gamification of security awareness training programs: A literature* [PhD Thesis, Doctoral dissertation, Georgia State University]. https://comp.mga.edu/static/media/doctoralpapers/2023_Tatum_0516152056.pdf

Yigit, Y., Kioskli, K., Bishop, L., Chouliaras, N., Maglaras, L., & Janicke, H. (2024). Enhancing Cybersecurity Training Efficacy: A Comprehensive Analysis of Gamified Learning, Behavioral Strategies and Digital Twins. *2024 IEEE 25th International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, 24–32. https://ieeexplore.ieee.org/abstract/document/10579129/

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. *Journal of Computer Information Systems*, *62*(1), 82–97. https://doi.org/10.1080/08874417.2020.1712269