# Cybersafe: Gamifying Cybersecurity Training with a Training App

**Carlos Roque[1], Gareth Moodley[2] and Sayonnha Mandal[2]**
[1]School of Engineering, UAGM Gurabo Campus, Puerto Rico
[2]College of Information Science and Technology, University of Nebraska Omaha, USA

croque16@email.uagm.edu
gmoodley@unomaha.edu
smandal@unomaha.edu

**Abstract:** The rapidly evolving digital landscape has triggered a surge in cybersecurity threats, particularly social engineering techniques which demand innovative and accessible countermeasures to combat them in an accessible and real-time format. We present "Cybersafe," a mobile application designed to empower users to identify and combat common social engineering exploits effectively. The transformative concept behind this initiative aims to reshape traditional cybersecurity training by introducing a gamified, user-friendly platform suitable for all age groups. Cybersafe's application's functionality revolves around interactive quizzes that assess users' ability to identify threats. The findings from the research serve as a valuable resource for cybersecurity trainers, application developers, and organizations striving for a secure digital environment.

**Keywords:** Cyber security, Mobile devices, Phishing, Social engineering,, Gamify, Vulnerability

## 1. Introduction

The rapidly evolving digital landscape has triggered a surge in cybersecurity threats, particularly social engineering techniques which demand innovative and accessible countermeasures to combat them in an accessible and real-time format. Current similar applications, such as NightHawk (Liu, et. al 2022) by PhishFort and GoPhish (Luse et. al, 2021), aim to actively prevent phishing by way of anti-phishing software and by assessing the security posture of enterprise employees trying to expose them to social engineering attacks. However, they both lack in teaching the user how to prevent phishing. They do not offer a set of instructions on how to observe behaviour from social inquiries, which can effectively plant ideas for end-users on how to catch a phishing attempt quickly and responsibly. Our app features a questionnaire-based approach categorized into different social engineering threats, where each question is assigned a specific weight. The user responds to the questions depending on the specific operational context and a cumulative score is assessed through the application to report the final threat likelihood score. Moreover, the app provides specific recommendations in a user-friendly format which enables the user to implement actionable items to change their practices. By adopting a gamified approach, Cybersafe intends to overcome the challenges of user engagement and retention typically associated with conventional training methods. The development and deployment of Cybersafe signifies a meaningful shift in cybersecurity training methods. Each question within the quiz holds a specific score and answering "yes" to a question indicates a potential vulnerability, subsequently increasing the total threat likelihood score. Broad questions are asked first, followed by more focused ones. Then, recommendations are shown that give the user actionable items to change their practices.

This scoring system serves to guide users in distinguishing genuine emails from phishing attempts, enhancing their cybersecurity skills progressively. The app also extends its learning scope to include web security, covering a broad spectrum of cybersecurity aspects to ensure comprehensive user awareness.

The paper further explores the developmental aspects of the Cybersafe application and provides an analysis of user feedback and learning outcomes. It concludes with a summary of findings and the potential impact of such a tool on global phishing prevention efforts.

## 2. Background

### 2.1 Business Email Compromise Attacks

The rising severity of phishing and other cyber threats is well documented. A 2019 report from the FBI highlighted the scale of the issue, suggesting that Business Email Compromise (BEC) attacks alone resulted in estimated damages of around 26 billion dollars. These attacks typically involve the impersonation of a business executive or an organization with the aim of tricking employees, partners, or customers into transferring money or sensitive data (Bakarich et. al., 2019).

### 2.2 COVID-Themed Phishing Lures

The threat has only escalated with recent global events such as the COVID-19 pandemic, which saw an increase in COVID-themed phishing lures. Cybercriminals quickly took advantage of the uncertainty and fear surrounding the pandemic, crafting deceptive emails and messages to trick users into revealing personal information or downloading malicious files.

### 2.3 Time Pressure Techniques

In addition, cybercriminals often employ "time pressure" psychological techniques in their attacks. These techniques create a sense of urgency that can cause users to react without taking the time to verify the legitimacy of the request. This further underscores the need for users to be educated about such tactics and the importance of verifying information before acting.

### 2.4 Risk-Taking

Risk-taking behaviour also plays a significant role in users' vulnerability to cyber threats. Users who are unaware of the risks associated with certain online behaviours, or who underestimate these risks, are more likely to fall victim to cyber-attacks (Aleroud et. al., 2017) .

The increasing sophistication and scale of these threats highlight the importance of tools like Cybersafe. By educating users on the risks and signs of phishing and other cyber threats, Cybersafe aims to reduce the likelihood of users falling victim to these attacks.

## 3. Adversary Motivations

Understanding the motivations of cyber attackers can provide valuable insights into the types of threats users may face and the tactics attackers may use. Common motivations include:

### 3.1 Financial Gain

One of the primary motivations for cyber-attacks is financial gain. Cybercriminals often target personal and financial information that can be used for fraudulent purposes or sold on the black market. Attacks like phishing and ransomware are typically financially motivated, aiming to trick users into providing sensitive information or paying a ransom (Abroshan et. al., 2021).

### 3.2 Information Stealing and Fraud

Cyber attackers may also be motivated by the desire to steal information. This can include personal data, business information, intellectual property, and even state secrets. The stolen information can be used for a range of malicious activities, from identity theft to corporate espionage (Chaudhary, 2016).

Fraud is another common motivation. Cybercriminals may impersonate legitimate entities to trick users into providing sensitive information or manipulate systems and transactions for illicit gain.

### 3.3 Spying Campaigns

Some cyber-attacks are part of broader spying campaigns, often conducted by state-sponsored actors. These attacks aim to gather intelligence on individuals, organizations, or nations for political or strategic purposes.

### 3.4 Political Motivations

Political motivations can also drive cyber-attacks. These can range from hacktivist campaigns aimed at promoting a political cause, to state-sponsored cyber warfare aimed at destabilizing or discrediting an adversary.

By understanding these motivations, Cybersafe can better equip users to recognize and respond to potential threats, reducing their risk of falling victim to cyber-attacks.

## 4. Related Research

Anti-phishing applications have been proposed and utilized since the beginning of phishing campaigns. Fairly recent research includes apps focused solely on email phishing (Helmi et. al., 2019), phishing using Wi-Fi hotspots (Chen et. al., 2021)) and specifically phishing on handheld mobile devices (Chorge et. al., 2016). Several efforts have been made to incorporate user awareness (Zieni et. al., 2023) components in phishing apps as well as apps dedicated primarily to educate users (Dixon et. al., 2019) regarding the various phishing and web exploits via different mediums (Lungu et. al., 2010). Applications such as MobiFish (Wu et. al., 2014) and NoPhish (Canova

et. al., 2014) have been proposed in prior research. For discussion in this section, we have identified at least two other similar candidates that attempt to prevent social engineering attacks and actively teach the user, these are: NightHawk by PhishFort, and GoPhish.

NightHawk, developed by PhishFort, is a robust platform specifically designed to combat phishing threats. It uses machine learning to automatically detect, analyse, and respond to phishing attacks in real time (Liu et. al., 2022). Users receive immediate alerts about potential threats and get comprehensive reports about each attack to deepen their understanding and improve future defence strategies. The operations for analysing URLs and detecting potential phishing links are performed at the backend of the app. The users are typically presented with a user interface with a custom watermark to denote that the URL is safe to proceed. The application lacks the ability to take the users step by step through the process of reasoning behind the final decision. The user only views the end user interface and the final recommendation. Hence, users remain unaware of potential phishing markers that are needed to identify similar future vulnerabilities. Moreover, NightHawk focuses more on the detection and immediate response part. Its user interface is designed for security teams rather than average internet users, which makes it less accessible for the public. On the other hand, Cybersafe emphasizes the educational element for the user to better understand social engineering attacks and potentially identify similar future attacks.

GoPhish is an open-source phishing toolkit designed for businesses and security professionals to test and enhance their organization's defences against phishing (Luse et. al., 2021). It allows users to create simulated phishing attacks to identify vulnerabilities within the organization. The tool then provides detailed reports about the simulation results to help educate the users and develop more effective strategies for real phishing attacks. GoPhish adopts a higher-level approach to scan and detect all potential phishing vulnerabilities in the users' systems. It provides a comprehensive analysis of user operations, such as, clicked URLs, data submitted, emails viewed, to provide the user with a view of their online activity and resultant exploits that they fell prey to. GoPhish's primary target audience is organizations rather than individual users, which contrasts with Cybersafe's emphasis on individual internet users. While both Cybersafe and GoPhish share the common goal of educating users about phishing attacks, their approaches differ significantly. GoPhish is a proactive tool aimed at training users through simulation, while Cybersafe is more reactive, focusing on real-time detection and education of users as threats occur.

In conclusion, while NightHawk and GoPhish bear similarities to Cybersafe, they differ in key aspects such as their target audience, usage approach, and primary focus. This makes Cybersafe a unique tool in its approach to preventing social engineering attacks and educating users.

## 5. Goals of Cybersafe

In an increasingly digital world, phishing attacks have become all too common, claiming many victims who lack the necessary knowledge to identify and avoid such threats. Users often inadvertently share sensitive information, such as login credentials or personal details, without recognizing the signs of a phishing attempt (Figure 1). This vulnerability is largely due to insufficient awareness or understanding of how phishing operates and the potential signs of an attack.

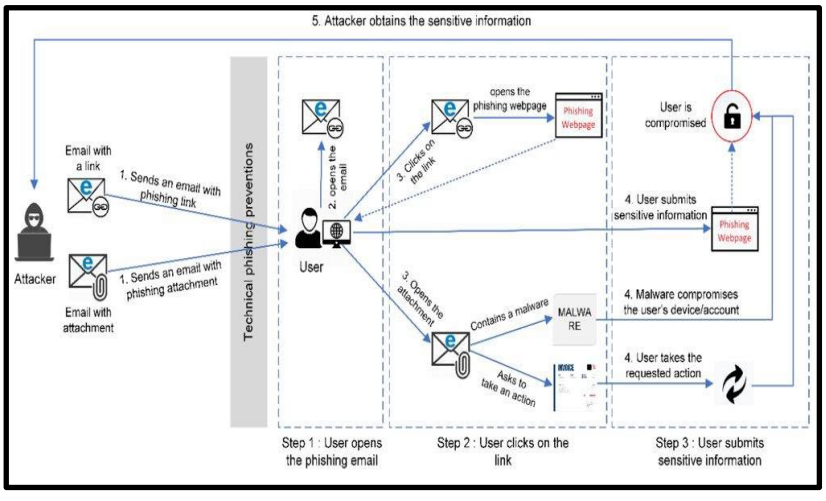


**Figure 1: Phishing Example**

### 5.1 Educating Users

Many users are not well-versed in basic browser and network security practices. This gap in knowledge can lead to risky behaviours, such as visiting unsecured websites or downloading unsafe files, which can expose users to various cybersecurity threats beyond phishing (Zieni, 2023). The primary goal of Cybersafe is to educate users on cybersecurity, equipping them with the knowledge and tools to better protect themselves online. By presenting information in a user-friendly format and providing personalized feedback based on each user's behaviour, Cybersafe aims to bridge the knowledge gap and help users develop safer online habits.

One of the key areas of focus is enabling users to recognize the signs of phishing emails. Cybersafe offers a detailed overview of common phishing tactics and provides real-time alerts when potential phishing attempts are detected. Furthermore, Cybersafe seeks to instil basic browser security methods as habits in users. Through interactive questionnaires and recommendations, users learn to identify unsecured websites, understand the importance of regularly updating browser software, and adopting secure practices like using strong, unique passwords. By addressing these critical areas of cybersecurity, Cybersafe is striving to empower users with the knowledge and habits they need to navigate the digital world safely and confidently.

### 5.2 The Gamified Approach

Cybersafe is a mobile application designed to help users become more aware of phishing attempts. It provides easy-to-understand and actionable information to guide users in recognizing and avoiding various types of cyber threats.

One of the unique aspects of Cybersafe is its use of gamification to teach users about various attacks. By turning learning into a game, Cybersafe makes the process of cybersecurity education more engaging and effective. Users can test their knowledge, track their progress, and even compete with friends to see who can achieve the highest Phishing Score.

The gamification component for Cybersafe is inspired from Yu-kai Chou’s Octalysis Framework (Chou, 2019). The Core Drives from the Framework that are primarily relevant to Cybersafe are Accomplishment, Empowerment, Avoidance and Unpredictability. The satisfaction and feeling of achievement by correctly identifying phishing markers and potential web vulnerabilities enable the user to feel empowered. The Black Hat core drives of Avoidance and Unpredictability also serve as strong drivers for users to engage and be motivated about solving potential phishing traps and enable them to feel a sense of control over their online safety requirements.

Cybersafe features a user-friendly interface that simplifies complex information about phishing. It breaks down technical jargon into understandable terms, making cybersecurity education accessible to users of all backgrounds and skill levels.

To ensure that users receive the most relevant and accurate information, Cybersafe uses comprehensive and up-to-date databases of known phishing websites and email addresses. These databases are continuously updated, providing users with real-time protection against emerging threats.

In addition, Cybersafe enables push notifications that alert users of potential phishing threats instantly. These real-time alerts give users the ability to act quickly, minimizing the chance of falling victim to phishing attacks.

Overall, Cybersafe provides a comprehensive and user-friendly solution to help individuals better understand and navigate the ever-evolving landscape of cyber threats.

## 6. Cybersafe

### 6.1 Operational Technology

Android Studio forms the primary development environment for the Cybersafe app. It's an industry-standard tool, offering a comprehensive suite of features to design and build applications for the Android operating system. Its range of developer tools and efficient code editor streamline the app-building process, making it easier to integrate with Android's wide array of features.

Apache Tomcat is an open-source implementation of various Java technologies that serves as the back-end server for Cybersafe. Tomcat's reliability, configurability, and strong community support make it a popular choice for building and deploying enterprise-grade applications. It handles the logic and server-side processes of the application, ensuring the smooth operation of Cybersafe's features.

Java 8 SDK is used for back-end programming in Cybersafe. Known for its versatility, robustness, and powerful feature set, Java 8 allows the application to effectively handle complex tasks. These tasks include analysing incoming data, detecting potential threats, and generating insightful educational content for the users.

Data storage in Cybersafe is managed by MySQL Database, a widely used and reliable relational database management system. MySQL facilitates efficient data storage, retrieval, and management. Its scalability and performance are critical in enabling the application to access and analyse vast amounts of data rapidly, an essential factor in detecting social engineering threats.

Servlets are employed in Cybersafe for handling requests and responses within the web environment. These server-side Java programs allow the application to extend its functionality, dynamically handling interactions with the user and ensuring efficient communication between the client and server.

Finally, Cybersafe utilizes RESTful APIs, with data structured in JSON for client-server communication. This technology promotes lightweight, stateless, and cacheable communication, boosting the overall performance and scalability of the application. Furthermore, RESTful APIs simplify the integration process with other systems and services, augmenting Cybersafe's versatility in combating social engineering attacks. We now discuss the specific operations provided by our Cybersafe application.

Cybersafe provides an array of functions designed to educate, warn, and protect users from various cybersecurity threats. The app uses a questionnaire format to assess user awareness and vulnerability to phishing, browser security, SMS phishing, and network security. These questionnaires provide valuable insights into user behaviours and facilitate personalized recommendations. The individual app functionalities are outlined below:

### *6.1.1 Phishing email detection*

- *Analyse Links:* Evaluates the links within emails to determine if they lead to known phishing sites.
- *Sender Requests PII:* Identifies requests for Personally Identifiable Information (PII) from unfamiliar senders.
- *Expectation:* Checks if the email aligns with the user's expectations or if it's unexpected and possibly suspicious.
- *Malicious Attachments:* Scans email attachments for known malicious code or signatures.

### *6.1.2 Browser security*

- *Public WIFI Network:* Alerts users when connected to public or unsecured WIFI networks.
- *Secure Site:* Checks for HTTPS in URLs to ensure the site encrypts user data.
- *Typos in URL or Page:* Identifies inconsistencies in URLs that could indicate a fake site.
- *Site Structure:* Analyses the overall structure of a site for signs of phishing.
- *Ads:* Monitors excessive or intrusive ads that might indicate a compromised or malicious site.
- *Browser Permissions:* Manages and monitors permission requests from websites to prevent unauthorized access to personal data.

### *6.1.3 SMS phishing*

- *Known Number:* Compares incoming SMS from numbers with known contact information.
- *Requests PII:* Detects requests for PII within SMS messages.
- *Secure Site:* Verifies that links within SMS lead to legitimate and secure sites.
- *Legitimate Site:* Checks for signs of legitimacy, such as contact info and privacy policies.

### *6.1.4 WIFI security*

- *Password Protected:* Ensures that the WIFI network is password protected.
- *WPA2/WPA3 Encryption:* Verifies the use of secure encryption protocols.
- *Known Users:* Monitors for unknown devices connected to the network.
- *VPN Use:* Encourages the use of Virtual Private Networks (VPNs) when appropriate.
- *Sensitive Info/Accounts:* Offers guidance on securing sensitive information and accounts when using public or shared networks.

Cybersafe's functions reflect a comprehensive approach to cybersecurity, offering robust protection across multiple domains. Its interactive and user-friendly design enables users to learn and apply cybersecurity best practices in their daily online activities, significantly reducing their risk of falling victim to cyber threats.

### 6.2 Operational Process for Cybersafe

Cybersafe's methodology starts with broad, general questions for each of its four categories: Email Phishing, Browsing Security, SMS Phishing, and Network Security. These questions establish a baseline understanding of the user's behaviours and potential vulnerabilities in each category. Each general question is then followed by a series of more targeted questions, which delve into specific behaviours and scenarios to gain a deeper understanding of the user's online habits.

The responses to both general and targeted questions are scored and combined to detect the likelihood of the user falling victim to phishing, spam, insecure browsing, or insecure network practices. This Phishing Score offers a quantitative measure of the user's risk level, providing an immediate insight into their current cybersecurity posture.

Based on the user's responses to both general and targeted questions, Cybersafe provides personalized recommendations. These recommendations address the specific behaviours and habits identified during the questionnaire process and provide the user with actionable advice on how to improve their online security. This approach ensures that the advice provided is relevant and helpful to each individual user, promoting a more effective learning experience and facilitating the adoption of safer online habits.

Through this combination of general and targeted questioning, scoring, and personalized recommendations, Cybersafe offers a comprehensive and personalized approach to cybersecurity education. The final operational database schema for Cybersafe is given in the appendix (Figure 2).

### 6.3 App Output

Cybersafe is designed to be a practical and dynamic tool that users can incorporate into their daily digital routines. When you receive an email, especially from an unfamiliar sender, use Cybersafe's phishing email detection feature. This tool analyses email for signs of phishing, such as unexpected requests for personal information, suspicious attachments, and unusual links. Like its email function, Cybersafe can also be used when receiving an SMS text message. It can detect messages from unknown senders, requests for personal information, and links to potentially dangerous sites.

Before browsing a new site, use Cybersafe's browser security function. This feature checks the site for secure connections (HTTPS), potential typos in the URL that could indicate a phishing attempt, and other signs of a secure and legitimate site.

When connecting to a new Wi-Fi network, Cybersafe's Wi-Fi security function can verify whether the network is password protected and using secure encryption protocols. It also encourages the use of a VPN when appropriate and offers guidance on securing sensitive information and accounts.

Cybersafe utilizes a unique methodology in the form of questionnaires to assess a user's vulnerability to different types of phishing and security threats. These questionnaires focus on four key areas: Email Phishing, Browsing Security, SMS Phishing, and Network Security. Each questionnaire is a mix of broad and narrow questions designed to gauge a comprehensive understanding of the user's security stance.

Through answering these questionnaires, users assist Cybersafe in grasping their online behaviours, potential threat exposure, and their comprehension of secure digital practices. This information is crucial in helping Cybersafe derive a "Phishing Score" for each user, indicating their overall risk of succumbing to phishing attacks.

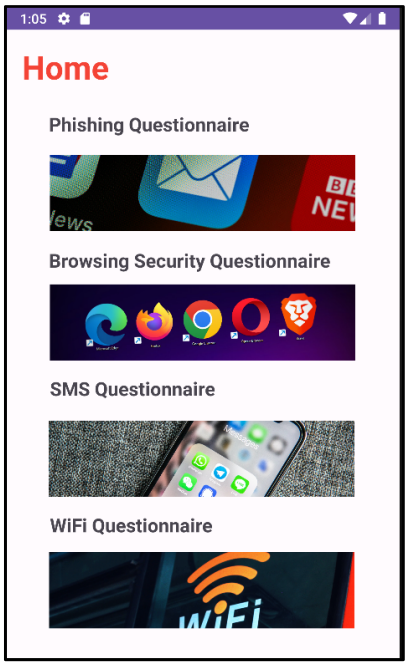


**Figure 3: Main menu of mobile application, to select type of questionnaire**

Each questionnaire is structured around a series of questions with three potential responses: "Yes", "No", or "Maybe". This allows users to give nuanced responses, effectively capturing their habits and potential vulnerabilities. When a user opts for "Maybe", they are encouraged to provide more context, giving further insights. Once completed, the questionnaire responses are evaluated to calculate the user's Phishing Score. A higher score represents a higher risk level.

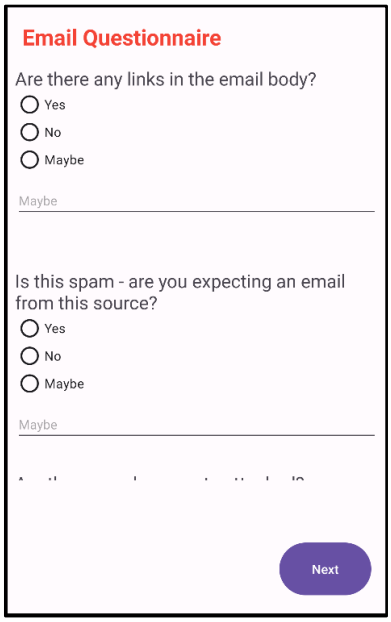


**Figure 4: Example questionnaire for Browser Security**

Beyond generating the Phishing Score, Cybersafe also offers personalized recommendations based on the user's questionnaire responses. These recommendations are specifically tailored around questions answered with "Yes", indicating potential security weak spots. The recommendations aim to educate users about these vulnerabilities and provide actionable steps to mitigate them.

This methodology of intertwining interactive questionnaires with personalized feedback allows Cybersafe to stand as an effective tool for increasing user awareness about social engineering threats and promoting safer online behaviours.

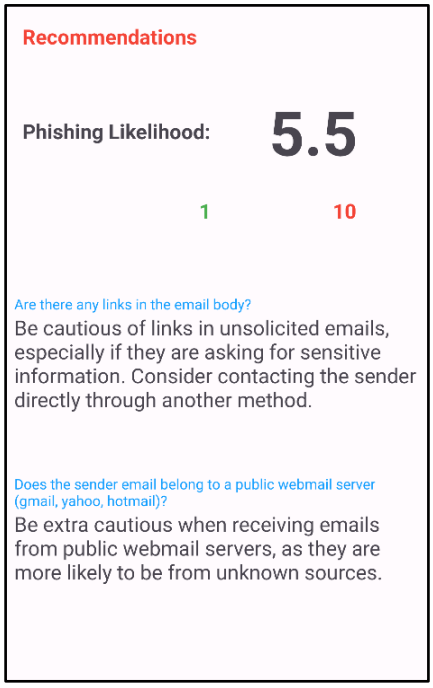


**Figure 5: Example recommendations for Browser Security questions**

With regular use of Cybersafe, users will enhance their ability to identify potential phishing attempts and other cybersecurity threats on their own. By integrating Cybersafe into daily online activities, users can gain practical experience in spotting and avoiding cyber threats, ultimately improving their cybersecurity skills and confidence.

## 7. Conclusion and Future Work

The lack of technological literacy among the public is a significant contributor to the growing prevalence and success of cyber-attacks. This gap in knowledge often leads to significant losses, both financial and personal, due to phishing and other forms of online fraud.

Cybersafe offers a solution to this issue by educating users about best practices in a personalized, engaging manner. By asking users about their online habits and providing specific questions and explanations in understandable vocabulary, Cybersafe makes cybersecurity education accessible to a wide audience.

As mobile devices continue to grow in popularity and become an increasingly common target for phishing and other cyber-attacks, it's crucial that phishing awareness and protection dynamics adapt to this change. By providing a mobile solution that users can easily incorporate into their daily routines, Cybersafe is helping to drive this adaptation, offering a relevant, user-friendly tool to enhance cybersecurity awareness and protection.

Cybersafe's goal is to empower individuals to navigate the digital world safely and confidently, thereby reducing the overall impact of cyber threats on our society. By making cybersecurity education a part of our daily online activities, we can turn the tide against cybercriminals and create a safer digital space for everyone.

As part of our future work, we plan to keep updating Cybersafe to include the latest phishing and web vulnerabilities as recorded by the cybersecurity community. This will ensure users obtain in-depth and relevant information about the current human-centric cyber threats.

Further, we plan to evaluate the usability, accuracy, and training effectiveness elements with user studies with community user participants. A pre and post evaluation measurement will be conducted to validate the usefulness of Cybersafe as an effective cybersecurity training tool and the extent of learning for the participants.

## References

Abroshan, Hossein, et al. "Phishing happens beyond technology: The effects of human behaviours and demographics on each step of a phishing process." *IEEE Access* 9 (2021): 44928-44949.

Aleroud, Ahmed, and Lina Zhou. "Phishing environments, techniques, and countermeasures: A survey." Computers & Security 68 (2017): 160-196.

Bakarich, K. M., & Baranek, D. (2020). Something phish-y is going on here: A teaching case on business email compromise. *Current Issues in Auditing*, *14*(1), A1-A9.

Canova, Gamze, et al. "NoPhish: an anti-phishing education app." Security and Trust Management: 10th International Workshop, STM 2014, Wroclaw, Poland, September 10-11, 2014. Proceedings 10. Springer International Publishing, 2014.

Chou, Y. K. (2019). *Actionable gamification: Beyond points, badges, and leaderboards*. Packt Publishing Ltd.

Chaudhary, Sunil. "The use of usable security and security education to fight phishing attacks." (2016).

Chen, Tianjun, Dexin Kong, and Yuxin Hong. "Development and implementation of anti phishing wi-fi and information security protection APP based on android." Journal of Physics: Conference Series. Vol. 1802. No. 3. IOP Publishing, 2021.

Chorghe, Sharvari Prakash, and Narendra Shekokar. "A survey on anti-phishing techniques in mobile phones." 2016 International Conference on Inventive Computation Technologies (ICICT). Vol. 2. IEEE, 2016.

Dixon, Matt, Nalin Asanka Gamagedara Arachchilage, and James Nicholson. "Engaging users with educational games: The case of phishing." Extended abstracts of the 2019 CHI conference on human factors in computing systems. 2019.

Helmi, Rabab Alayham Abbas, et al. "Email Anti-Phishing Detection Application." 2019 IEEE 9th International Conference on System Engineering and Technology (ICSET). IEEE, 2019.

Lungu, Ion, and Alexandru Tăbușcă. "Optimizing Anti-Phishing Solutions Based on User Awareness, Education and the Use of the Latest Web Security Solutions." Informatica Economica14.2 (2010).

Liu, Zhe, et al. "Nighthawk: fully automated localizing UI display issues via visual understanding." *IEEE Transactions on Software Engineering* 49.1 (2022): 403-418.

Luse, Andy, and Jim Burkman. "Gophish: Implementing a Real-World Phishing Exercise to Teach Social Engineering." *Journal of Cybersecurity Education, Research and Practice*2020.2 (2021): 5.

Wu, Longfei, Xiaojiang Du, and Jie Wu. "MobiFish: A lightweight anti-phishing scheme for mobile phones." 2014 23rd international conference on computer communication and networks (icccn). IEEE, 2014.

Zieni, Rasha, Luisa Massari, and Maria Carla Calzarossa. "Phishing or not phishing? A survey on the detection of phishing websites." *IEEE Access* 11 (2023): 18499-18519.

## Appendix

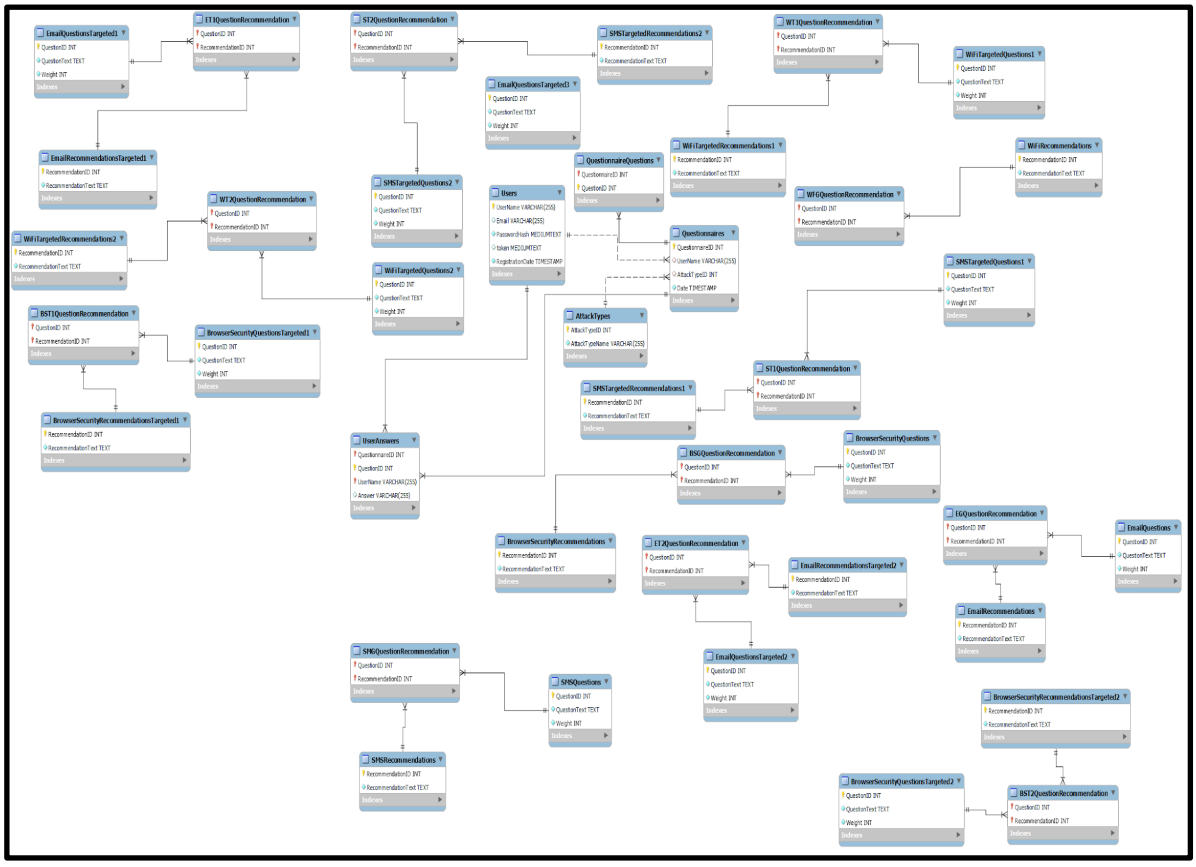

**Figure 2: Final Database Schema Diagram**