4-2024

# ENHANCING CYBERSECURITY AWARENESS IN THE UNITED ARAB EMIRATES: AN ASSESSMENT OF CURRENT PRACTICES AND THE DEVELOPMENT OF AN AI-ENHANCED MOBILE APPLICATION

Meera Humaid Alalawi
*United Arab Emirates University*

جامعة الإمارات العربية المتحدة
United Arab Emirates University

MASTER THESIS NO. 2024: 7

College of Information Technology

Department of Information Systems and Security

# ENHANCING CYBERSECURITY AWARENESS IN THE UNITED ARAB EMIRATES: AN ASSESSMENT OF CURRENT PRACTICES AND THE DEVELOPMENT OF AN AI-ENHANCED MOBILE APPLICATION

*Meera Humaid Alalawi*

*April 2024*

United Arab Emirates University

College of Information Technology

Department of Information Systems and Security

# ENHANCING CYBERSECURITY AWARENESS IN THE UNITED ARAB EMIRATES: AN ASSESSMENT OF CURRENT PRACTICES AND THE DEVELOPMENT OF AN AI-ENHANCED MOBILE APPLICATION

Meera Humaid Alalawi

This thesis is submitted in partial fulfilment of the requirements for the degree of Master of Science in Information Security

March 2024

**United Arab Emirates University Master Thesis**
**2024: 7**

Cover: Enhancing Cybersecurity Awareness in the United Arab Emirates

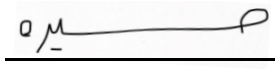
(Photo: By Meera Humaid Alalawi)



Print: University Print Service, UAEU 2024

## Declaration of Original Work

I, Meera Humaid Alalawi, the undersigned, a graduate student at the United Arab Emirates University (UAEU), and the author of this thesis entitled "*Enhancing Cybersecurity Awareness in the United Arab Emirates: An Assessment of Current Practices and the Development of an AI-Enhanced Mobile Application*", hereby, solemnly declare that this is the original research work done by me under the supervision of Dr. Saed Al Rabaee in the College of Information Technology at UAEU. This work has not previously formed the basis for the award of any academic degree, diploma or a similar title at this or any other university. Any materials borrowed from other sources (whether published or unpublished) and relied upon or included in my thesis have been properly cited and acknowledged in accordance with appropriate academic conventions. I further declare that there is no potential conflict of interest with respect to the research, data collection, authorship, presentation and/or publication of this thesis.

Student's Signature: 

Date: __ April 18, 2024 _____

## Advisory Committee

1) Advisor: Dr. Saed Alrabaee

Title: Associate Professor

Department of Information Systems and Security

College of Information Technology

2) Member: Prof. Khaled Shuaib

Title: Professor

Department of Information Systems and Security

College of Information Technology

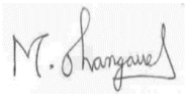
# Approval of the Master Thesis

This Master Thesis is approved by the following Examining Committee Members:

1) Advisor: Dr. Saed Alrabaee
   Title: Associate Professor
   Department of Information Systems and Security
   College of Information Technology

   Signature  Date April 07, 2024

2) Member: Dr. Thangavel Murugan
   Title: Assistant Professor
   Department of Information Systems and Security
   College of Information Technology

   Signature  Date April 15, 2024

3) Member (External Examiner): Dr. Issam Al Azzoni
   Title: Associate Professor
   Department of Software Engineering
   Institution: College of Engineering, Al Ain University of Science and Technology, Al Ain, UAE

   Signature  Date April 15, 2024

This Master Thesis is accepted by:

Acting Dean of the College of Information Technology: Dr. Fekri Kharbash

Signature 

Date 20/05/2024

Dean of the College of Graduate Studies: Professor Ali Al-Marzouqi

Signature 

Date 23/05/2024

# Abstract

In today's interconnected world, individuals, private corporations, public institutions, and governments face increasingly sophisticated cyber threats and attacks, highlighting the critical need for individuals and organizations to understand cybersecurity comprehensively. Cyberattacks have affected many countries and infrastructures in different sectors worldwide, including the United Arab Emirates (UAE), which has become a main target for cybercrime due to its booming economy and tourism. The UAE considers cybersecurity an increasingly critical issue in our digital world, and increasing cybersecurity awareness among residents is essential to protect themselves and their organizations from cyberattacks. The primary objectives of this study are to identify key challenges and gaps in school cybersecurity curricula and university program outcomes, evaluate the current state of cybersecurity awareness among individuals in the UAE through a survey, and develop an AI-enhanced mobile application to address the identified cybersecurity awareness gaps among individuals in the UAE. The study's results identified gaps in the Ministry of Education's (MoE) curriculum for grades 1 to 12 in UAE public schools, highlighting a need for more direct, in-depth cybersecurity education to equip students with the skills to navigate evolving cyber threats. Additionally, while UAE universities offer a range of cybersecurity programs, challenges persist in aligning these curricula with international standards, ensuring practical experience, and updating content to reflect the latest cyber threats. The cybersecurity awareness survey further uncovered diverse levels of understanding and various practices among UAE residents, pointing out huge misconceptions and inconsistent cybersecurity practices. These findings underscore the urgent need for enhanced cybersecurity education and practices. In response, an AI-enhanced mobile application was developed to address these gaps tailored to each individual's unique needs, offering tailored cybersecurity education content, including news updates, a roadmap for certifications, interactive tasks and quizzes, etc. Utilizing AI, the app provides personalized responses and assistance, fostering a more informed and secure digital environment for UAE residents.



**Keywords**: Cybersecurity, Awareness, Education, Mobile Application, Artificial Intelligent.

# Title and Abstract (in Arabic)

## تعزيز الوعي بالأمن السيبراني في دولة الإمارات العربية المتحدة: تقييم الممارسات الحالية وتطوير تطبيق الهاتف المحمول المعزز بالذكاء الاصطناعي


***الملخص***

في عالم اليوم المترابط، يواجه الأفراد والشركات الخاصة والمؤسسات العامة والحكومات تهديدات وهجمات سيبرانية متطورة بشكل متزايد، مما يسلط الضوء على الحاجة الماسة للأفراد والمنظمات لفهم الأمن السيبراني بشكل شامل. أثرت الهجمات الإلكترونية على العديد من البلدان والبنى التحتية في مختلف القطاعات في جميع أنحاء العالم، بما في ذلك دولة الإمارات العربية المتحدة، التي أصبحت هدفًا رئيسيًا للجرائم الإلكترونية بسبب ازدهار اقتصادها وسياحتها. تعتبر دولة الإمارات العربية المتحدة الأمن السيبراني قضية بالغة الأهمية في عالمنا الرقمي، كما أن زيادة الوعي بالأمن السيبراني بين السكان أمر ضروري لحماية أنفسهم ومؤسساتهم من الهجمات السيبرانية. تتمثل الأهداف الأساسية لهذه الدراسة في تحديد التحديات والفجوات الرئيسية في مناهج الأمن السيبراني المدرسية ونتائج البرامج الجامعية، وتقييم الوضع الحالي للوعي بالأمن السيبراني بين الأفراد في دولة الإمارات العربية المتحدة من خلال استطلاع، وتطوير تطبيق جوال معزز بالذكاء الاصطناعي لمعالجة فجوات الوعي بالأمن السيبراني بين الأفراد في دولة الإمارات العربية المتحدة. وحددت نتائج الدراسة فجوات في مناهج وزارة التربية والتعليم للصفوف من الأول إلى الثاني عشر في المدارس الحكومية في دولة الإمارات العربية المتحدة، مما سلط الضوء على الحاجة إلى تعليم مباشر ومتعمق أكثر للأمن السيبراني لتزويد الطلاب بالمهارات اللازمة للتعامل مع التهديدات السيبرانية المتطورة. بالإضافة إلى ذلك، في حين تقدم جامعات الإمارات العربية المتحدة مجموعة من برامج الأمن السيبراني، لا تزال هناك تحديات في مواءمة هذه المناهج مع المعايير الدولية، وضمان الخبرة العملية، وتحديث المحتوى ليعكس أحدث التهديدات السيبرانية. وكشف استطلاع التوعية بالأمن السيبراني أيضًا عن مستويات متنوعة من الفهم والممارسات المختلفة بين المقيمين في دولة الإمارات العربية المتحدة، مما يشير إلى مفاهيم خاطئة كبيرة وممارسات غير متسقة في مجال الأمن السيبراني. تؤكد هذه النتائج على الحاجة الملحة لتعزيز تعليم وممارسات الأمن السيبراني. واستجابة لذلك، تم تطوير تطبيق جوال معزز بالذكاء الاصطناعي لمعالجة هذه الفجوات ومصمم خصيصًا لتلبية الاحتياجات الفريدة لكل فرد، وتقديم محتوى تعليمي مخصص للأمن السيبراني، بما في ذلك تحديثات الأخبار، وخريطة طريق للشهادات، والمهام التفاعلية والاختبارات، وما إلى ذلك. وباستخدام الذكاء الاصطناعي، يوفر التطبيق استجابات ومساعدة شخصية، مما يعزز بيئة رقمية أكثر استنارة وأمانًا للمقيمين في دولة الإمارات العربية المتحدة.



**مفاهيم البحث الرئيسية**: الأمن السيبراني، التوعية، التعليم، تطبيق الهاتف المحمول، الذكاء الاصطناعي.

# Acknowledgements

I extend my deepest gratitude to Dr. Saed Alrabaee for his invaluable guidance, support, and mentorship throughout this research journey. His expertise in cybersecurity, keen insights, and constructive feedback have been instrumental in shaping this thesis. Dr. Alrabaee's unwavering encouragement and belief in my capabilities have motivated me to pursue excellence and navigate the challenges of this study. I also extend my heartfelt gratitude to Nisha Thorakkattu Madathil, Simon Darota, and Winner Abula for their invaluable support in the development of the mobile application. Collaborating with such a dedicated and skilled team has enriched this project immeasurably. Their contributions, commitment, and teamwork have been pivotal to the success of this work. I am deeply appreciative of their hard work and support, which have made this experience both rewarding and productive. I am profoundly thankful for the opportunity to work under Dr. Alrabaee's supervision and for his significant contribution to my academic growth, as well as the invaluable support from Nisha, Simon, and Winner, which has been instrumental in the successful development of our mobile application.

# Dedication

*To my beloved family and friends*

# Table of Contents

Title ..... i
Declaration of Original Work ..... iii
Advisory Committee ..... iv
Approval of the Master Thesis ..... v
Abstract ..... vii
Title and Abstract (in Arabic) ..... viii
Acknowledgements ..... ix
Dedication ..... x
Table of Contents ..... xi
List of Tables ..... xv
List of Figures ..... xvi
List of Abbreviations ..... xviii
Chapter 1: Introduction ..... 1
1.1 Overview ..... 1
1.2 Problem Statement ..... 2
1.3 Research Questions ..... 3
1.4 Research Objectives and Contributions ..... 4
1.5 Thesis Organizations ..... 4
Chapter 2: Literature Review ..... 6
2.1 Background ..... 6
2.1.1 Cybersecurity Attacks ..... 6
2.1.1.1 Overview of Cybersecurity Attacks ..... 6
2.1.1.2 Strategies and Motivations of Cyber Attackers ..... 8
2.1.1.3 Types of Cyber Attacks ..... 11
2.1.1.4 Cyber Attack Incidents in the UAE ..... 15
2.1.2 Cybersecurity Awareness ..... 18
2.1.2.1 Global Cybersecurity Awareness ..... 18
2.1.2.2 Cybersecurity Awareness in the UAE ..... 20
2.2 Related Works ..... 22
2.2.1 Cybersecurity Awareness Applications and Games ..... 22
2.2.2 AI in Cybersecurity Education ..... 30

Chapter 3: Research Methodology ..... 36
3.1 Research Framework ..... 36
3.2 Phase 1: Identify Cybersecurity Education and Curriculum Gaps ..... 38
3.2.1 Plaining ..... 38
3.2.2 Data Collection ..... 38
3.2.3 Data Analysis ..... 38
3.2.4 Identified Gaps ..... 39
3.3 Phase 2: Cybersecurity Awareness and Best Practices in the UAE ..... 39
3.3.1 Survey Design ..... 39
3.3.2 Participation Selection ..... 39
3.3.3 Survey Distribution ..... 40
3.3.4 Data Collection ..... 40
3.3.5 Data Analysis ..... 40
3.3.6 Synthesizing Findings ..... 40
3.4 Phase 3: Comprehensive Synthesis ..... 41
3.5 Phase 4: Mobile Application Development ..... 41
3.5.1 Planning and Analysis ..... 41
3.5.2 Design and Prototyping ..... 42
3.5.3 Software Development ..... 42
3.5.4 Testing ..... 42
3.5.5 Deployment ..... 42
3.5.6 Maintenance and Updates ..... 43
3.6 Phase 5: Research Results ..... 43
Chapter 4: Cybersecurity Education Gap Identification in the UAE ..... 44
4.1 Curriculum Gap Identification in the Public Schools in the UAE ..... 44
4.1.1 Current State of Cybersecurity Education ..... 44
4.1.2 Identified Gaps and Their Implications ..... 48
4.2 Gap Identification in Universities Cybersecurity Programs in the UAE ..... 49
4.2.1 Overview of Current Cybersecurity Programs ..... 49
4.2.2 Identified Gaps and Challenges Based on International Standards ..... 56
Chapter 5: Cybersecurity Awareness Study in the UAE ..... 58
5.1 Participant Demographics ..... 58
5.2 Survey Findings ..... 60

5.2.1 Knowledge and Awareness of Cybersecurity ..... 60
5.2.2 Cybersecurity Practices and Beliefs ..... 66
5.2.3 Experiences with Cybersecurity Threats ..... 71
5.2.4 Learning Preferences ..... 72
5.3 Discussion ..... 73
Chapter 6: Comprehensive Synthesis ..... 76
6.1 Key Findings and Major Concerns ..... 76
6.2 User Categorization and Cybersecurity Awareness Needs ..... 77
6.2.1 Individuals Aged Under 18 ..... 78
6.2.1.1 School Students Under the Age of 14 ..... 78
6.2.1.2 School Students Between the Ages of 14 and 18 ..... 78
6.2.2 Individuals Aged Above 18 ..... 79
6.2.2.1 University Students, Graduates, Unemployed ..... 79
6.2.2.2 Employees ..... 79
Chapter 7: Development of An AI Mobile Application ..... 81
7.1 Analysis ..... 81
7.2 Design and Development ..... 82
7.2.1 Users Login / Sign up Page ..... 82
7.2.2 Application User Categories (My Learning Page) ..... 84
7.2.2.1 Users Aged under 18 ..... 84
7.2.2.2 Users Aged above 18 ..... 87
7.2.3 Evaluation Tests and Grades ..... 89
7.2.4 Home Page Features ..... 89
7.2.4.1 Security News ..... 90
7.2.4.2 Security Certifications Roadmap ..... 90
7.2.4.3 Report Cybercrimes ..... 91
7.2.4.4 Social Media Privacy and Security (Tips and Recommendations) ..... 92
7.2.4 AI Assistant ..... 92
7.3 System Design ..... 93
7.3.1 Front-End Development ..... 93
7.3.2 Back-End Development ..... 94
7.4 Testing ..... 94
Chapter 8: Conclusion ..... 95

8.1 Summary of the Key Findings ..... 95
8.2 Challenges and Limitations ..... 95
8.3 Future Research Directions ..... 96
References ..... 98

# List of Tables

Table 1: Hacker types, motivations, and their strategies .....10
Table 2: Common types of malware attacks.....12
Table 3: Common types of social engineering attacks .....13
Table 4: Common types of network attacks .....14
Table 5: Common types of web-based attacks .....15
Table 6: Summary of cyber incidents in the UAE.....16
Table 7: Recent studies focusing on gamification for cybersecurity awareness .....26
Table 8: Mobile application to enhance cybersecurity awareness.....29
Table 9: AI in enhancing cybersecurity awareness.....33
Table 10: ACC-Accredited Active Cybersecurity-Related Programs in the UAE .....55

# List of Figures

Figure 1: Cybercrime Cost Estimation from 2018 to 2027 ..... 7
Figure 2: IC3 Report-2022 and Report-2020 Cybercrime Attack Types ..... 8
Figure 3: Research Framework ..... 37
Figure 4: Number of Participants per Emirates ..... 58
Figure 5: Participants Age and Gender ..... 59
Figure 6: Participants Occupational Status ..... 60
Figure 7: “I know what information security, or cybersecurity, means” ..... 60
Figure 8: "Which of the following is the best definition of cybersecurity?" ..... 61
Figure 9: "Where did you first hear about cybersecurity?" ..... 62
Figure 10: “I am aware that strong passwords must include” ..... 62
Figure 11: "I am aware that passwords need to be changed every" ..... 63
Figure 12: “What is phishing?” ..... 64
Figure 13: "Which of the following is an example of a phishing attack?" ..... 65
Figure 14: "What is malware?" ..... 65
Figure 15: "What is a firewall?" ..... 66
Figure 16: "I don't trust any file I receive from people I don't know" ..... 67
Figure 17: "I trust and open any unexpected file I receive from people I know" ..... 67
Figure 18: "It is safe to enter your private info on a site that starts with "http:// "" ..... 68
Figure 19: "What is the most secure action to take?" ..... 69
Figure 20: Participants' Responses to a Potential Phishing Attempt Scenario ..... 69
Figure 21: Participants' Behavior in Handling the Found USB Device ..... 70
Figure 22: Identifying Trustworthy Online Shopping Websites ..... 70
Figure 23: Cybersecurity Incidents Encountered by Participants/Their Family Members ..... 71
Figure 24: Learning Preferences ..... 72
Figure 25: Application Overview Structure ..... 82
Figure 26: Login/Sign Up Page ..... 83
Figure 27: Beginning Test ..... 83
Figure 28: “My Learning” Pages (Users Under 18 in the Middle, Above 18 in the Right) ..... 84

Figure 29: Example of Video Content for Users Under the Age of 18 .....85
Figure 30: Example of Story Content for Users Under the Age of 18 .....86
Figure 31: Example of Scenario Content for Users Under the Age of 18 .....87
Figure 32: Example of Lesson Content for Users Above the Age of 18 .....87
Figure 33: Example of Lesson Content for Employee Users .....88
Figure 34: Evaluation Tests and Grades .....89
Figure 35: Security News Page.....90
Figure 36: Security Certifications Roadmap .....91
Figure 37: Report Cybercrimes Page.....91
Figure 38: Social Media Privacy and Security .....92
Figure 39: GPT-API Integration .....93

# List of Abbreviations

| | |
|---|---|
| AI | Artificial Intelligent |
| CCDI | Computing Creative Design Innovation |
| MoE | Ministry of Education |
| NLP | Natural Language Processing |
| UAE | United Arab Emirates |

# Chapter 1: Introduction

## 1.1 Overview

In the digital age, technology has become more widespread and integrated into our day-to-day lives, and individuals need to maintain a comprehensive understanding of cybersecurity. The term "cybersecurity" has become a significant and critical concern for individuals, organizations, and governments worldwide. Sensitive personal data faces several multifaceted challenges that are not easily overcome, especially with the massive growth of interconnected devices, including cyber-attacks, insider threats, lack of awareness, weak policies and procedures, data breaches, increased data collection, and use of third-party services. The continued growth of generating data from digital technologies in the world has led to the emergence of big data, which allows cybercriminals to seek to exploit vulnerabilities in order to steal sensitive data. Therefore, cybersecurity threats become more complex for individuals and organizations, highlighting the need to embrace cybersecurity measures and education to protect these data. The National Institute of Standards and Technology (NIST) emphasized the critical need for organizations to implement and adopt the best practices to assess and protect personally identified information from cyber-attacks [1].

The United Arab Emirates (UAE) recognizes cybersecurity as a crucial issue in today's digital era and acknowledges the growing need for cybersecurity education. This initiative aims to equip the upcoming generation with essential skills and knowledge in cybersecurity to tackle cyberattacks and protect the UAE's digital infrastructure [2]. The Minister of Education emphasized the transformative potential of technology in education, stating, "Rather than think of technology as a tool to overcome a crisis, we should view it as a means to transform education" [3]. The extensive use of several technologies, such as computers in education, has led to the emergence of next-generation educational technologies, including Artificial Intelligence (AI) in education, which utilizes data processing and analytics to enable human-like cognition and functionalities, promoting new functionalities in education, such as academic and learning performance prediction, learning path recommendation, and teaching strategy optimization [4]. The UAE has embraced the National Strategy for AI as part of its Centennial 2071 plan; UAE's vision

by 2031 is to be one of the leading global nations in AI and focus on employing AI in several key areas, including the education sector [5], [6]. Therefore, adopting AI can assist in enhancing cybersecurity education and awareness in the UAE. Given the increasing reliance on technology in various life aspects, including education, it is crucial for UAE residents, especially students, to understand the fundamentals of cybersecurity. Lack of cybersecurity awareness can lead to severe consequences, such as identity theft or data breaches, making it crucial for individuals to protect their sensitive personal information from cyberattacks. Besides the education sector, it is also crucial to educate employees about cybersecurity, as they are the weakest vulnerable link in each organization. Cybersecurity is not considered only a technological issue but also a sociotechnical issue. Employees can inadvertently expose their organizations to cyber threats by falling victim to social engineering attacks, clicking on phishing emails, or using weak passwords. Moreover, with the increase in remote work, employees use their devices to access organizational data, increasing the risk of cyberattacks. Therefore, enforcing cybersecurity policies, educating employees about cybersecurity best practices, and keeping employees updated on the latest security threats are necessary to minimize the cybersecurity threats in each organization [7].

### 1.2 Problem Statement

The unprecedented interconnectivity and technological advancements in our digital world have increased cybersecurity attacks and concerns; however, many individuals and organizations in the UAE lack adequate cybersecurity awareness, leaving them vulnerable to cyber threats. Cybersecurity awareness can be attributed to various factors, including gaps in cybersecurity curricula in UAE schools and universities. These programs may cover only some aspects of cybersecurity, leaving students ill-prepared to deal with evolving threats. Furthermore, traditional teaching methods may not effectively convey the necessary information, resulting in students not fully comprehending the importance of cybersecurity in our daily lives. This leads to them being unable to respond to cyber threats effectively. On the other hand, many organizations fail to implement appropriate cybersecurity measures, which is considered a concerning issue. The lack of cybersecurity awareness and cybersecurity best practices causes organizations to be vulnerable to various cybersecurity issues, such as data breaches and ransomware attacks, which expose

organizations to substantial financial losses and reputational damage and put employees' sensitive data at risk. In recent years, the UAE has experienced a notable surge in cyber assaults, particularly amidst the COVID-19 pandemic, because of the unprecedented rise in digital interconnectivity among individuals. During the pandemic, several cyberattacks and malware targeted individuals and organizations in the UAE. According to [8], the severity of the cyber threat is highlighted by recent data and trends, which show a global increase of 50% in cyberattacks in 2021 compared to 2020. In the UAE, the growth was even higher, at 71%. During the fourth quarter of 2021, there were an average of 925 cyber-attacks per week per organization globally, compared to 408 cyberattacks in the UAE. In 2020, the UAE saw a 250% increase in cyberattacks during the pandemic, including 1.1 million phishing attacks, the most common technique for ransomware attacks. Ransomware attacks also increased, with over 33% of new threat groups affecting 78% of UAE organizations in 2020. While the percentage of UAE organizations hit by ransomware in 2021 decreased by 59%, the impact and damage caused by these attacks were still substantial [9]. Thus, the frequency of cyber assaults directed towards the UAE underscores the necessity of augmenting cybersecurity awareness among individuals to establish adequate protection mechanisms and defenses.

### 1.3 Research Questions

The problem statement clearly indicates a critical need for improved cybersecurity awareness in the UAE. This study aims to evaluate the current cybersecurity awareness practices in the UAE and explore the potential of an AI-enhanced mobile application to provide an innovative approach to cybersecurity education. The research questions have been carefully formulated to systematically address the different facets of this endeavour, focusing on assessing the current practices, identifying gaps, and leveraging AI technology to enhance cybersecurity awareness among individuals in the UAE. The main research questions are as follows:

1. What is the current state of cybersecurity awareness among individuals in the UAE?
2. How effective are the UAE's cybersecurity awareness programs and initiatives to mitigate cyber threats?

3. What are the key challenges and gaps in the current cybersecurity curricula in the UAE?
4. How can AI be leveraged to enhance cybersecurity awareness and education in the UAE?
5. What are the design and functional requirements for an AI-enhanced mobile application aimed at improving cybersecurity awareness in the UAE?
6. What impact does the use of an AI-enhanced mobile application have on the cybersecurity awareness levels of users in the UAE?

## 1.4 Research Objectives and Contributions

This thesis aims to address the research questions concerning enhancing cybersecurity awareness in the UAE by delineating clear objectives. The main objectives are the following:

1. To assess and evaluate the current state of cybersecurity awareness among the individuals in the UAE through a knowledge assessment study to assess individuals' awareness levels and understanding of cybersecurity concepts and best practices.
2. To identify the key challenges and gaps in the cybersecurity curricula and programs currently offered by schools and universities in the UAE.
3. To explore the potential of AI technologies to enhance cybersecurity awareness and education, looking at innovative methods to integrate AI into learning processes.
4. To design and develop an AI-enhanced mobile application specifically tailored to improve cybersecurity awareness in the UAE, considering user engagement and the effectiveness of educational content.

## 1.5 Thesis Organizations

The thesis is meticulously organized to ensure a coherent and comprehensive exploration of enhancing cybersecurity awareness in the UAE through an AI-enhanced mobile application. It begins with an introduction in Chapter 1, where the topic, problem statement, research questions, objectives, and contributions are outlined. Chapter 2 delves

into the literature review, bifurcated into background and related works. The research methodology is detailed in Chapter 3, explaining the data collection and analysis approach. Chapter 4 identifies the gaps in cybersecurity curriculum at schools and universities in the UAE. Chapter 5 presents the results of a cybersecurity awareness study. A comprehensive synthesis in Chapter 6 summarizes key findings from the previous two chapters and outlines the requirements for developing the AI-enhanced mobile application, which is fully described in Chapter 7. The thesis concludes with Chapter 8, summarizing the study's contributions, limitations, and directions for future research.

# Chapter 2: Literature Review

This chapter thoroughly examines the current state of cybersecurity awareness, with a particular focus on the United Arab Emirates (UAE). The aim is to investigate the changing landscape of cybersecurity threats, the effectiveness of existing awareness programs, and the potential of AI-enhanced mobile applications in cybersecurity education. The research will cover global and UAE cybersecurity trends, common cyberattacks, the role of AI in cybersecurity education, and existing mobile applications in cybersecurity. The review will highlight the increasing reliance on technology and the importance of human factors in cybersecurity. This study aims to identify research gaps, particularly in developing and implementing practical cybersecurity awareness tools in the UAE. This will pave the way for further exploration of AI-enhanced cybersecurity educational solutions.

## 2.1 Background

### *2.1.1 Cybersecurity Attacks*

#### *2.1.1.1 Overview of Cybersecurity Attacks*

Cybersecurity plays a vital role in preserving the integrity, confidentiality, and availability of information in our digital world and protecting our systems, networks and data from unauthorized entities, attacks, or damages. Nevertheless, the growth in volume and complexity of interconnected devices introduced an evolution in malicious cyber-attacks, leading to substantial security risks in cyberspace. Organizations have deployed monitoring systems in order to protect organization assets, such as firewalls, password management, data leak prevention and constant network monitoring. However, these technical solutions are insufficient to provide full protection against cybersecurity attacks because many users are unaware of cybersecurity policies or do not comply with the organization’s information security policies [10], [11].

The concept of cyberattacks is defined in various ways, each with its own focus and limitations. One perspective is that cyberattacks are actions undertaken by nations to infiltrate and disrupt or damage other countries' computer systems, but this fails to account for attacks by individuals or non-state groups. Another definition describes them as any

intentional efforts to disrupt or destroy the computer networks of another country, which is too broad and doesn't distinguish between cybercrime, cyberattack, and cyberwarfare. A different viewpoint highlights digital attacks that result in systems producing false responses, but this excludes a range of threats to national security. Lastly, there's a definition based on the consequences of an attack, like causing physical harm or property damage, focusing more on the outcomes than the nature of the attack itself. Each of these definitions contributes to understanding cyberattacks but does not fully capture the entire scope of these threats [12]. Therefore, cyberattacks are a set of tactics carried out by a group or single individuals who can exploit vulnerabilities in computer systems, networks, and devices over the Internet with the intention of damaging or accessing and viewing sensitive data; often, they are motivated by personal motives, political activity, or financial gain. Accordingly, as illustrated in Figure 1, the estimated cybercrime cost will increase to higher than $23 trillion by 2027 [13], [14].

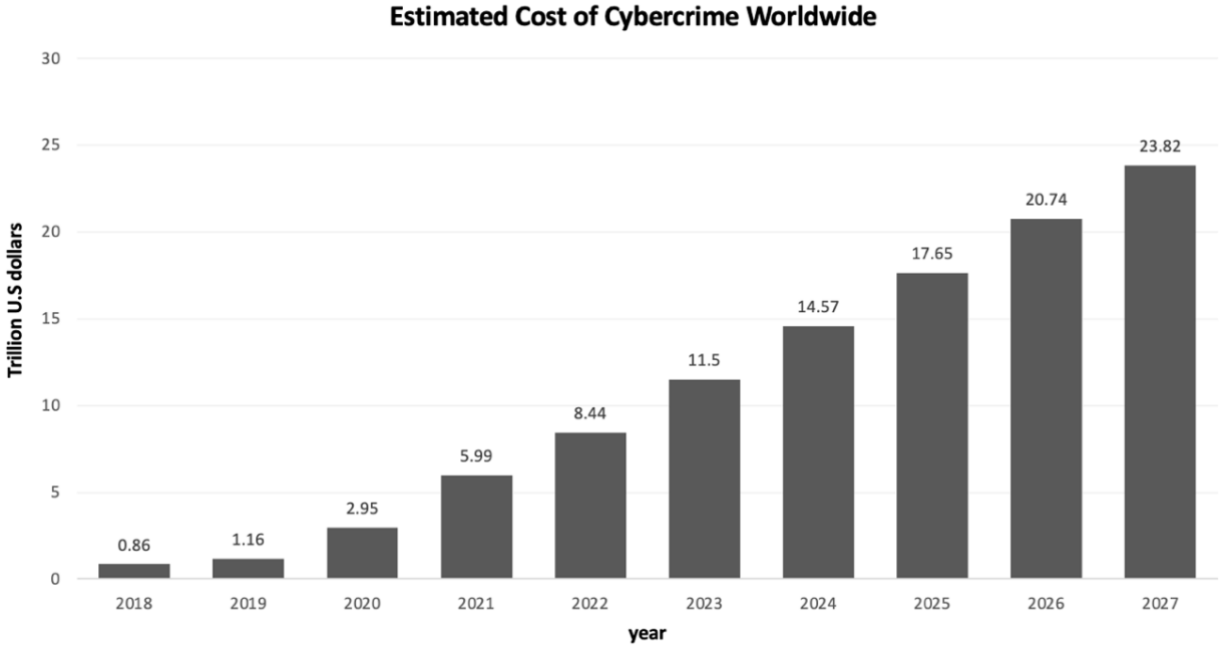



Figure 1: Cybercrime Cost Estimation from 2018 to 2027

Cybersecurity and cybercrime problems affect individuals and organizations at all levels and threaten privacy, personal security, financial health, and national security [15]. According to [16] the Internet Crime Complaint Center (IC3) 2022 report issued by the lead U.S. Federal Bureau of Investigation (FBI) revealed a total loss of $27.6 Billion from

3.26 million complaints from the year 2018 to 2022, which represents a substantial increase compared with the revealed report in 2020 [17] were the total loss is $13.3 Billion from 2.21 million total complaints. Figure 2 represents the complaints of cybercrime types from the released IC3 reports for 2020 and 2022. In 2022, the top four crimes were phishing, personal data breach, non-payment or non-delivery, and extortion, with phishing being the most prevalent, impacting over 300,000 victims. Comparatively, in 2020, the leading crimes were quite similar; phishing, vishing, smishing, and pharming had the highest number of victims, followed by non-payment, non-delivery, extortion, and personal data breaches. Phishing-related victims increased significantly, from approximately 241,000 in 2020 to over 300,000 in 2022. There are also notable shifts in other crime types, such as government impersonation and overpayment scams, which appear in the 2020 list but are absent from the 2022 data. Conversely, crimes like tech support, identity theft, and employment-related fraud remain common in both years, although their ranking by victim count varies.

**2022 Crime Types**

**By Victim Count**

| *Crime Type* | *Victims* | *Crime Type* | *Victims* |
|---|---|---|---|
| Phishing | 300,497 | Government Impersonation | 11,554 |
| Personal Data Breach | 58,859 | Advanced Fee | 11,264 |
| Non-Payment/Non-Delivery | 51,679 | Other | 9,966 |
| Extortion | 39,416 | Overpayment | 6,183 |
| Tech Support | 32,538 | Lottery/Sweepstakes/Inheritance | 5,650 |
| Investment | 30,529 | Data Breach | 2,795 |
| Identity Theft | 27,922 | Crimes Against Children | 2,587 |
| Credit Card/Check Fraud | 22,985 | Ransomware | 2,385 |
| BEC | 21,832 | Threats of Violence | 2,224 |
| Spoofing | 20,649 | IPR/Copyright/Counterfeit | 2,183 |
| Confidence/Romance | 19,021 | SIM Swap | 2,026 |
| Employment | 14,946 | Malware | 762 |
| Harassment/Stalking | 11,779 | Botnet | 568 |
| Real Estate | 11,727 | | |

**2020 Crime Types**

**By Victim Count**

| Crime Type | Victims | Crime Type | Victims |
|---|---|---|---|
| Phishing/Vishing/Smishing/Pharming | 241,342 | Other | 10,372 |
| Non-Payment/Non-Delivery | 108,869 | Investment | 8,788 |
| Extortion | 76,741 | Lottery/Sweepstakes/Inheritance | 8,501 |
| Personal Data Breach | 45,330 | IPR/Copyright and Counterfeit | 4,213 |
| Identity Theft | 43,330 | Crimes Against Children | 3,202 |
| Spoofing | 28,218 | Corporate Data Breach | 2,794 |
| Misrepresentation | 24,276 | Ransomware | 2,474 |
| Confidence Fraud/Romance | 23,751 | Denial of Service/TDoS | 2,018 |
| Harassment/Threats of Violence | 20,604 | Malware/Scareware/Virus | 1,423 |
| BEC/EAC | 19,369 | Health Care Related | 1,383 |
| Credit Card Fraud | 17,614 | Civil Matter | 968 |
| Employment | 16,879 | Re-shipping | 883 |
| Tech Support | 15,421 | Charity | 659 |
| Real Estate/Rental | 13,638 | Gambling | 391 |
| Advanced Fee | 13,020 | Terrorism | 65 |
| Government Impersonation | 12,827 | Hacktivist | 52 |
| Overpayment | 10,988 | | |

Figure 2: IC3 Report-2022 [16] and Report-2020 [17] Cybercrime Attack Types

### *2.1.1.2 Strategies and Motivations of Cyber Attackers*

In recent years, the escalating sophistication of cybercriminal strategies has made it increasingly difficult for victims to detect warning signs and significantly hindered the identification of the perpetrators and their motives [18]. Cybercrime involves attacking internet-connected devices or computers to make a profit by accessing the user's data for

personal gain. The perpetrator of this crime is known as a hacker and is usually highly skilled in interfering without their knowledge with the personal data of internet users. Usually, the goal of hackers is to benefit themselves financially. For instance, they may use hacking algorithms to crack the code of banking websites, log in to a user's account, and withdraw all the available funds to their own account. In some cases, organizations may use hacking to gain a competitive advantage over their rivals by accessing confidential information such as budgets, investment plans, and details of projects or new plans. Alternatively, an individual hacker may attempt to gain control of a user's banking credentials to withdraw money into their own account [19].

However, the world of cybercrime is vast and varied, with numerous types of hackers and a range of motivations driving their actions. These include script kiddies, cyberpunks, insiders, petty thieves, grey hats, professional criminals, hacktivists, and nation-states. The motivations behind their activities are diverse, with curiosity, financial gain, notoriety, revenge, recreation, and ideology being the most common. Each hacker or group of hackers has developed unique strategies and methods for launching attacks, ranging from basic hacking tools to sophisticated nation-state attacks.

"Script kiddies", or novice hackers, are beginners using existing scripts for hacking; they are often driven by curiosity or a desire for notoriety. "Cyberpunks" are hackers with a rebellious attitude towards authority and the status quo, often motivated by a desire to challenge systems and sometimes driven by ideological stances. "Insiders" are individuals with legitimate access to an organization's systems but misuse their privileges for personal gain or to cause harm. "Petty thieves" engage in cybercrime for financial gain. They are often involved in credit card fraud, identity theft, or other types of financial scams, while "professional criminals" from organized crime groups conduct sophisticated attacks usually aimed at large-scale financial gain or revenge. "Hacktivists" use their skills to support political or social causes, often targeting opposing organizations. Finally, "nation-state" hackers, supported by governments, engage in espionage, sabotage, or cyber warfare to influence global events. Table 1 Summarizes hacker types, motivations, and strategies [18]-[24].

Table 1: Hacker types, motivations, and their strategies

| Types | Motivations | Strategies |
|---|---|---|
| Script Kiddies | Curiosity, Notoriety, Recreation | Launch attacks without specific provocation, often targeting victims arbitrarily. They typically operate solo, using basic equipment and freely available online tools to identify and exploit system vulnerabilities. While they can affect vulnerable networks, their lack of advanced tools limits their impact on well-secured systems. |
| Cyberpunks | Financial, Notoriety, Revenge, Recreation | Initiate attacks without specific triggers but are drawn to prominent targets like military or government entities. They possess a moderate skill level with a general understanding of software, hardware, and programming. Often, they own some basic specialized equipment and may exchange information in niche online forums or within hacking collectives; typically adopt internet-sourced tools for their needs. |
| Insiders | Financial, Revenge, Ideology | Often motivated by negative work experiences, typically target their current or former workplaces using their in-depth knowledge and access. Their attacks, considered highly skilled due to insider information, usually involve sabotage, intellectual property theft, or fraud, exploiting their trusted position. |
| Petty Thieves | Financial, Revenge | Execute cyberattacks without specific provocation, with moderate skill levels tailored towards their goals rather than technological curiosity. They adapt to digital methodologies as their traditional targets shift online, acquiring the requisite skills for effective attacks. Opting for anonymity to safeguard their operations, they usually avoid active participation in hacking circles. Despite financial constraints, they often have the necessary specialized tools for their illicit activities. |
| Grey Hats | Curiosity, Notoriety, Recreation, Ideology | Drawn to high-security and challenging targets, often seeking sensitive information. They possess high-level skills, including specialized knowledge in computer and network security. While typically working alone, Grey Hats actively share knowledge and leverage advanced tools developed by their peers. Their methods range from exploiting known vulnerabilities to creating new zero-day attacks. Generally, they cause minimal damage to systems, although they might steal and disclose select data. |
| Professional Criminals | Financial, Revenge | Approach cyber activities with a calculated, professional mindset, not needing specific triggers to act. They rigorously assess risks against potential rewards, focusing on targets with promising financial outcomes. With advanced computer security and crimeware skills and deep knowledge of their target areas, they operate in structured, business-like networks with specialized roles and resources. Their significant financial backing allows them to make sizeable investments if the potential returns are substantial. |
| Hacktivists | Notoriety, Revenge, Recreation, Ideology | They display varied skill levels and are driven by ideological motives but often include highly skilled core members. Notable groups like "Anonymous" even run training programs to enhance member skills. Despite financial constraints, these groups boast large memberships, granting access to specialized information and the ability to launch impactful attacks like DDoS attacks, sometimes extending to physical activism and commonly exploiting known vulnerabilities, such as SQL injection, to gain access to and publicize sensitive data. |

Table 1: Hacker types, motivations, and their strategies (Continued)

| Types | Motivations | Strategies |
|---|---|---|
| Nation States | Financial, Revenge, Ideology | Usually prompted by geopolitical conflicts, with these actors possessing extremely high skills backed by the resources of an entire nation. They typically have access to abundant funding, superior equipment, and extensive intelligence, surpassing other hacker groups. Nation States often operate covertly online, targeting nationally significant resources like critical infrastructure. Their strategies often involve a blend of social engineering, spear-phishing, and advanced trojans. |

Understanding the motivation behind hackers' activities is essential for effective cybersecurity management. Hackers have varied motives, such as curiosity, financial gain, notoriety, revenge, recreation, and ideology, influencing their methods and targets, as represented in Table 1. By comprehending these motivations, organizations can tailor their defense strategies, anticipate potential threats, and respond more effectively to incidents. This knowledge aids in prioritizing resources, shaping security policies, and educating employees about specific risks. Furthermore, it assists in legal and diplomatic responses, especially in state-sponsored cyberattacks.

*2.1.1.3 Types of Cyber Attacks*

Cybersecurity attacks fall into two primary categories: passive and active attacks, each with distinct characteristics and impacts. Passive attacks are characterized by their non-intrusive nature. The attackers observe, monitor, or use information from a system but do not alter or affect the system's resources or data for instance, eavesdropping on network traffic and accessing messages without authorization. The stealthy nature of passive attacks makes them hard to detect, as they leave the system's information and resources unchanged. Their primary objective is to gather information, such as scanning for open ports and identifying network vulnerabilities. In contrast, active attacks are more intrusive and involve altering or modifying system data, which impacts the system's resources. These attacks, such as Denial of Service (DoS) attacks and trojans, can cause direct damage to the victims. Active attacks often follow passive attacks, where the attacker first gathers necessary information covertly before launching the more overt active attack. Victims are usually aware of active attacks due to their disruptive nature. These attacks

pose a significant threat to the integrity and availability of systems and are generally more complex to execute than passive attacks [25].

Cybersecurity attacks are complicated because attackers use advanced techniques and tools to bypass firewalls and antivirus programs to exploit computer systems and networks. Common types of cyberattacks include malware attacks, social engineering attacks, network attacks, web-based attacks, system-based attacks, and application attacks.

Malware Attacks: short for malicious software, refers to any software designed with harmful intent. Its purposes range from disrupting normal operations and circumventing access restrictions to collecting sensitive data, presenting unwelcome ads, or seizing device control without the user's consent. Additionally, malware and software that cause unintentional harm are categorized as bad ware. Key types of malwares include viruses, worms, Trojans, ransomware, spyware, etc [26]. Table 2 presents the common types of malware attacks.

Table 2: Common types of malware attacks

| Attack | Description |
|---|---|
| Viruses | A computer virus is designed to replicate or clone itself, often damaging or compromising other programs on the host's system. Typically, it requires some form of human intervention to effectively spread or reproduce itself [27]. |
| Worms | A worm differs from a virus by its ability to self-replicate and spread across computer networks without any external assistance, functioning independently [27]. |
| Trojans | A Trojan horse is harmful software that masquerades as legitimate or hidden in legitimate software. To the unaware user, these programs may appear beneficial, intriguing, or seemingly innocuous, but they can cause damage upon execution [28]. |
| Ransomware | Encrypts files and documents on systems ranging from individual PCs to entire networks, including servers. Victims typically face limited options: they can pay the ransom to the cybercriminals to regain access to their encrypted network, attempt to restore their data from backups, or hope for the availability of a free decryption key [29] . |
| Spyware | Refers to any program or software secretly installed on a person's computer, often restricting the user's intended actions. Typically, the user remains unaware of the presence of this spyware [27]. |
| Adware | A form of software that is capable of automatically presenting or downloading advertising content to a user without their consent while they are online [30]. |

Social Engineering Attacks: refers to manipulative techniques that exploit human psychology to gain unauthorized access to information or systems. These attacks leverage the natural tendency of people to trust others, making humans the weakest link in security chains. Social engineering attacks are grouped into human-based and computer-based types. Human-based attacks involve direct personal interaction to collect information, affecting fewer victims. Computer-based attacks, such as those using the Social Engineering Toolkit for spear phishing, use technology like computers or phones to quickly target a larger number of victims. These attacks can also be classified based on their social, technical, or physical approach. Each type exploits different vulnerabilities, ranging from personal relationships in social attacks to exploiting online platforms in technical attacks and direct physical actions in physical-based attacks [31]. Common social engineering attacks mentioned in Table 3.

Table 3: Common types of social engineering attacks

| Attack | Description |
|---|---|
| Phishing | An attack that aims to deceive individuals into obtaining sensitive data such as passwords, credit card numbers, and personal details, which often involves using fraudulent emails that appear to be from trustworthy sources, such as well-known websites, platforms or banks, to gain the victim's trust. These emails typically contain deceptive links that mimic legitimate websites, tricking victims into unwittingly providing their information [32]. |
| Spear Phishing | Targets specific individuals or organizations by sending emails tailored to appear as though they come from a known associate to increase the likelihood of deceiving the recipient into following the sender's instructions. The content of the email is crafted to seem relevant and legitim to the target, containing personalized information gathered from social media platforms like LinkedIn such as the target's name and specific data to avoid suspicion [31]. |
| Smishing (SMS Phishing) | This form of phishing involves sending texts to victims with a fraudulent URL. The message, disguised as coming from a legitimate source, prompts the recipient to send personal information or download a malicious app [31]. |
| Vishing (Voice Phishing) | This form of phishing involves sending texts to victims with a fraudulent URL. The message, disguised as coming from a legitimate source, prompts the recipient to send personal information or download a malicious app [31]. |
| Pretexting | A traditional form of social engineering in which the attacker acquires confidential or sensitive information from victims through fabricated scenarios, either in person or through communication channels, typically over the phone. This tactic may take different forms, e.g., pretending to ask for help or impersonating technical support to obtain information [33]. |

Table 3: Common types of social engineering attacks (Continued)

| Attack | Description |
|---|---|
| Baiting | involves an attacker placing a device, like a USB drive, loaded with malware in a spot where it's likely to be discovered and used, initiating the attack once the victim engages [33]. |
| Quid Pro Quo | Perpetrators pose as tech support over the phone to infiltrate a company's network under the guise of resolving an issue and then plant a virus or malware. Often, these attackers exfiltrate personal data and demand payment, typically in cryptocurrency [34]. |
| Piggybacking | When someone with legitimate access inadvertently allows an unauthorized individual entry, often by holding a secure door open, either out of a desire to help or simply due to politeness. This can occur in large organizations where employees might not recognize all their colleagues [33]. |
| Shoulder Surfing | Occurs when an attacker gains information by covertly watching over the victim's shoulder, such as by observing the entry of usernames and passwords on a computer or inspecting sticky notes and papers, particularly when the victim is not paying attention [33]. |
| Dumpster Diving | Involve collecting confidential materials from a company's waste or disposed items, including outdated computer components, drives, CDs, and DVDs [31]. |

Network Attacks: malicious activities intended to interfere with, harm, or gain unauthorized access to computer networks and the associated devices. These attacks specifically target the protocols and infrastructure of networks and exploit vulnerabilities that can be used for various malicious purposes. presents the common types of network attacks.

Table 4: Common types of network attacks

| Attack | Description |
|---|---|
| Denial-of-Service (DoS) attack | Overwhelming the bandwidth or resources of a target machine or network to prevent legitimate users from accessing the service; it involves a single machine [35]. |
| Distributed Denial of Service (DDoS) attacks | The attacker takes control of multiple computers, often spread across different locations (forming a botnet) and uses them to flood the target with an overwhelming volume of traffic [35]. |
| Man-in-the-middle (MitM) Attacks | The attacker positions themselves as an intermediary between a client and a router to either passively observe the traffic or actively alter the messages being communicated, which compromises the confidentiality and integrity of the messages sent between the client and the router [36]. |
| Session Hijacking | Involves an attacker impersonating a legitimate client to gain unauthorized access to a network connection. This type of attack is executed by combining techniques from MITM and DoS attacks, enabling the attacker to assume the identity of a legitimate user and hijack their session [37]. |

Web-Based Attacks: Web-based attacks refer to a category of cyber threats that target vulnerabilities in websites or web applications. These attacks exploit weaknesses in the web platform to achieve various malicious objectives, such as compromising data integrity, stealing information, or disrupting normal web functionalities. Table 5 presents the common types of web-based attacks.

Table 5: Common types of web-based attacks

| Attack | Description |
|---|---|
| SQL Injection | A web application security flaw where attackers exploit application code to access or tamper with database contents. When successful, this vulnerability enables the attacker to manipulate the database by creating, reading, updating, or deleting data stored in the connected backend system [38]. |
| Cross-Site Scripting (XSS) | Targets a user's application by embedding client-side scripts, like JavaScript, into a web application's output which allows attackers to modify the client-side script of a web-based application. As a result, attackers can execute these scripts in the victim's browser, leading to potential outcomes like redirecting users to malicious websites [38]. |
| Cross-site request forgery (CSRF) | An attacker tricks a user into visiting a trusted server through a malicious URL. This enables the attacker to inject their own authorization code into the server [39]. |

Finally, AI-driven cyberattacks refer to malicious activities in cybersecurity that utilize AI to enhance their effectiveness. This involves using AI algorithms to automate attack processes, make them more adaptable, and improve their ability to evade detection. These attacks can be more sophisticated and targeted, making them harder to defend against. AI-driven cyberattacks might include advanced phishing attacks, automated exploitation of vulnerabilities, intelligent malware, or AI-powered network intrusions. AI allows attackers to quickly analyze vast amounts of data, adapt to changing environments, and make decisions with minimal human intervention. Therefore, AI can be used to manipulate data, leading to incorrect categorization or interpretation by AI systems. AI can create realistic, but fake, data like images, audio, or text. This can deceive humans and AI systems by generating fake news or deep-fake videos. AI's advanced data analysis capabilities can be exploited for malicious purposes, like identifying vulnerabilities or predicting system responses to certain attacks [40]-[42].

#### *2.1.1.4 Cyber Attack Incidents in the UAE*

Cyberattacks affected many countries worldwide, including UAE, which has become a significant target for cybercrime due to its booming economy and tourism. In

the UAE, identity theft usually occurs in the banking sector, where attackers steal users' sensitive data to initiate transactions and steal money from existing users' accounts. Moreover, 85% of the population in the UAE uses the internet and social media, which increases the spread of cyber victimization. Cyberattacks increased in the UAE by 71% in 2021 compared to 2020. The average of cyberattacks facing organizations per week is 925 during the fourth quarter of 2021 compared to 408 in 2020 including 1.1 million phishing attack attempts. Organizations in the UAE faced ransomware assaults, and it affected 78% of the organizations in 2020 compared to 66% in 2019 [43]. According to [8], the percentage of organizations hit by ransomware attacks in 2021 in the UAE is 59%, and the encryption rate is 46%. The average ransom payment in the UAE organizations is $225.338, and the average cost to rectify the incident is $1.26 million, which is a 144% rise compared to 2020. Cyberattack incidents in the UAE have significantly impacted diverse sectors such as government, energy, transportation, healthcare, education, and telecommunications. Table 6 provides a summary of the notable cyberattack incidents that have occurred in the UAE.

Table 6: Summary of cyber incidents in the UAE

| Year | Cyberattacks | Targeted Sector | Description |
|---|---|---|---|
| 2023 | LockBit Ransomware [44] | Various sectors | LockBit's strategy centred around double extortion, involving files/data encryption and threats to leak publicly the stolen sensitive data if ransoms weren't paid. |
| 2022 | Conti Ransomware [44] | Various sectors | Encrypting files and demanding a ransom; if the ransom was not paid, the stolen data was threatened to be sold or published. |
| 2019 | ZeroCleare Wiper [45] | Industrial and Energy | Overwrites critical components such as the Master Boot Record (MBR) on Windows systems, resulting in severe data loss and rendering the systems inoperable. |
| 2019 | Snatch Ransomware [44] | Various sectors | Forcing infected hosts to reboot into Safe Mode to gain initial access, extract sensitive data and ransom demands. |
| 2018 | DNS hijacking [46] | Various sectors | Attackers manipulated DNS records to redirect visitors of legitimate websites to malicious sites. |

Table 6: Summary of cyber incidents in the UAE (Continued)

| Year | Cyberattacks | Targeted Sector | Description |
|---|---|---|---|
| 2017 | Shamoon [47] | Oil and Gas, Transportation and Government | Shamoon uses network credentials to distribute a dropper across connected systems containing multiple harmful subcomponents. One key component is a wiper, which destroys data on the infected systems. |
| 2016 | Targeted attack (Operation Ghoul) [48] | Industrial and Engineering companies | A spear-phishing campaign to extract sensitive data using HawkEye malware in deceptive emails to collect sensitive data for financial gain. |
| 2015 | Adwind RAT malware [49] | Various sectors | Extract sensitive data and control users' computers |
| 2015 | Trojan Laziok [48] | Government (Energy) | Used for reconnaissance and data extraction from targeted computers. It spread through spam emails with Microsoft Excel attachments. Upon clicking these attachments, the Trojan began its infection, compromising the systems. |

As we have observed, the escalating prevalence of cybersecurity issues globally and the rising incidence of cybercrime underscore the critical need for heightened awareness and proactive measures among users. Key cybercrimes such as phishing, non-payment/non-delivery, extortion, and personal data breaches continue to proliferate, highlighting the imperative for user vigilance. Moreover, the rapid evolution of cybercriminal strategies and techniques necessitates ongoing education and awareness efforts to empower users to confront emerging threats effectively. Various forms of cyberattacks, including malware, social engineering, network, web-based, and AI-driven attacks, pose significant risks to users who lack awareness of their actions. Like many other regions, the UAE has witnessed numerous incidents affecting organizations and individuals, as detailed in Table 6. However, the adverse impact of such incidents can be mitigated by fostering cybersecurity awareness and adherence to best practices. Therefore, it is paramount to prioritize efforts to enhance cybersecurity awareness globally and within the UAE specifically. By equipping users with the knowledge and tools necessary to navigate the evolving cybersecurity landscape, we can strengthen our collective defenses against cyber threats and effectively protect our digital environments.

### *2.1.2 Cybersecurity Awareness*

#### *2.1.2.1 Global Cybersecurity Awareness*

Cybersecurity awareness has been described as the extent to which users comprehend the significance of securing information, along with their duties and actions required to maintain adequate information security measures for protecting an organization's data and networks [50]. Researchers emphasized that while IT professionals can implement various controls to protect electronic information, it is the authorized end users who possess the access credentials (IDs and passwords) and have the power to print, share, alter, or delete data. The risk lies in the fact that if these users are careless with their passwords, discard confidential information improperly, neglect virus scanning, or leave data backups unsecured, then the information remains at risk. Software and hardware security mechanisms can only be effective if users consistently follow certain security practices [51]. Therefore, it has been observed that there is a general lack of awareness regarding cyber threats, which include the use of apps and the sharing of information on social networks and web pages. Crucially, it's noted that hackers, whether working alone or in groups, often target the most vulnerable users—those who lack information and network security awareness. These hackers exploit software flaws and security weaknesses that users inadvertently introduce [50].

Security is an essential aspect of software products, and it becomes even more important when children are involved. Cybersecurity is one of the most critical areas when considering security in this context. The security and privacy of children have been a concern for researchers in the child computer interaction (CCI) research community. Among the challenges identified by this community, one significant issue is the impact of social and cloud technologies on CCI, which brings risks to children's privacy and security. These risks have become a part of children's daily lives as they grow up immersed in technology much more than previous generations could have imagined. Children are increasingly active internet users and are quickly becoming more familiar with the technology. As a result, the popularity of the Internet and social networks among children is rising. Children could face various risks: content risks, contact risks, children targeted as consumers, economic risks, and online privacy risks. Content risks were further divided

into illegal content, harmful or age-inappropriate content, and harmful advice related to alcohol, drugs, suicide, and psychological or nutritional disorders [52].

A study by [53] assessed internet usage and cybersecurity awareness among New Zealand students aged 8 to 21 years. The study, which covered both computers and mobile devices, revealed a general lack of cybersecurity awareness, with the lowest awareness observed in the 8-12 year age group, who could only answer 19% of the questions. Most students were not only unfamiliar with basic cybersecurity terms but also lacked awareness of common threats like phishing and cybersecurity tools for tablets and smartphones, which are essential for students with the increase in e-learning and Bring Your Own Device (BYOD) initiatives in the education system. Furthermore, researchers examined the level of cyber security knowledge among college students and found that many students needed better cyber security awareness; many were unaware of how to protect their data and of cyber security risks, such as malware-infected websites and phishing attacks. Researchers emphasized the need for improved cyber security awareness and training programs among college students to ensure they can effectively protect their personal data and mitigate cyberattack risks [54].

Research has been conducted to better understand the general public's attitude, knowledge, behavior, and other relevant factors regarding cybersecurity awareness. One study found that cybersecurity awareness among the general public in the Kingdom of Saudi Arabia (KSA) needs to be improved, which may be related to the country's cultural nature. Another study conducted an online survey to evaluate the cybersecurity awareness of individuals in the same country. The participants had good knowledge of information technology, but their awareness of cybercrime threats, cybersecurity practices, and the role of government and organizations in ensuring information safety on the internet needed to be improved. To understand the level of information security awareness among employees of educational institutions in the Middle East, a study revealed that not all employees had adequate knowledge and understanding of information security principles and their practical applications. As a result, it was recommended that comprehensive awareness and training programs be implemented at all levels of the institutions to prevent negative consequences for the institutions and their employees [55].

A study was conducted by [56] to measure the level of cybersecurity awareness in terms of cybercrime risk awareness among students in the Kyrgyz Republic; it revealed that despite numerous reports on computer crimes available online, there is a notable lack of awareness and understanding of cybercrime among students. The study analyzed how information security awareness relates to the students' computer literacy and field of study. It was concluded that even though information technology is extensively used, there is a critical need for education on information security topics to protect individuals from becoming victims of cybercrime.

Another study conducted by [57], focusing on cybersecurity awareness in Bangladesh, found disjointed and inadequate awareness of cybercrime among the population. The findings showed that most of the public lacks awareness of essential cybersecurity practices, highlighting a substantial gap in knowledge and understanding of this critical issue. Furthermore, the study pointed out that the government of Bangladesh and related organizations have been insufficiently proactive and effective in tackling and mitigating cybercrime-related issues.

A study conducted by [58] focusing on Malaysian undergraduate students discovered that out of 295 participants, more than one-third had fallen victim to scams on Social Networking Sites (SNS). On the other hand, an investigation was carried out by the Department of Computer Science at Yobe State University in Nigeria [59], focusing on assessing students' cybersecurity knowledge and internet usage behavior. The analysis of the experiment's results revealed that cybersecurity awareness among university students is moderately satisfactory, but most of them lack adequate knowledge on how to protect their personal data.

#### *2.1.2.2 Cybersecurity Awareness in the UAE*

The Internet plays a crucial role in the daily life of the UAE, as the country ranks among the top worldwide in terms of individual Internet usage. It has been observed that there has been a noticeable rise in internet users in Middle Eastern countries in recent years, with the UAE experiencing a particularly steep increase. This surge is in line with the UAE government's continuous efforts to attain the highest standards of technological advancement [60], [61]. However, as reported by the UAE Cyber Security Centre, the

UAE is the second most targeted country for cyberattacks globally. This high frequency of attacks is attributed to the country's widespread internet use, technological advancement, and significant international presence, leading to an estimated annual cybercrime cost of around $1.4 billion [62]. Complementing this, a study by [62] analyzed cyber activity and perceptions in the UAE, benchmarking them against nine developed countries. The study found that the UAE's monetary losses from cybercrime, in relation to perceived risk, are comparable to those of countries like Canada. Although the UAE may lag behind these nations in terms of digital maturity, internet access, and cybersecurity awareness, its patterns of cyber risk behavior are similar. This parallel underscores the UAE's critical need for enhanced cybersecurity awareness programs.

A study conducted by [63] assessing school teachers' awareness of student cybersecurity in Ajman, UAE, involved a survey of 172 teachers across 29 private schools. The results showed an increase in teacher awareness in 13 aspects of student cybersecurity but a decrease in eight others, with a notable correlation between the teachers' specialization and cybersecurity awareness—mathematics and social science teachers displayed higher awareness levels than Arabic and English language teachers. Despite high internet access among UAE school students, the study found that teacher awareness about cybersecurity is only moderately sufficient, particularly lacking knowledge of safe internet use policies and responses to cybersecurity issues, likely due to inadequate training. Consequently, the research recommends incorporating cybersecurity education into the UAE school curriculum, emphasizes the need for regular cybersecurity training for teachers, aims to improve student safety online and reduce cybercrime risks, and suggests future studies to develop cybersecurity curriculum models for students.

Another study was conducted by [64] to evaluate students' e-security behaviours at a prominent higher education institution in the UAE, focusing on malware, password usage, data handling, phishing, social engineering, and online scams. Utilizing the E-Security Behavior Survey Instrument (EBSI) alongside focus group discussions, the study assessed the students' computing practices. The findings indicate moderately positive overall e-security behavior among these students. Specifically, their behaviours were favourable in areas such as phishing, social engineering, and online scams but showed uncertainty in dealing with malware, password management, and data handling. Contrary

to other studies that reported unsatisfactory results in students' e-security behaviors, this study found that while students exhibit good practices in certain aspects, their uncertain behaviors in others still leave them vulnerable to security risks.

Thus, the studies conducted in the UAE and other countries confirm that the lack of cybersecurity awareness is a global issue, indicating a concerning trend of inadequate knowledge and understanding of cyber threats. This underscores the universal necessity for improved cybersecurity education and strategic measures; it is crucial to increase awareness among individuals to prevent cyberattacks against individuals and organizations. Educating people about the risks and best practices of cybersecurity can help them become more aware and take preventive measures to protect themselves and their organizations. This awareness can also help individuals, including children, school and university students, and employees, to recognize common types of cyberattacks, such as phishing schemes and malware, and to learn how to identify and respond to them effectively.

To summarize, researchers have highlighted various issues individuals face with social and cloud technologies, including risks to children's privacy and security, such as content risks. Studies conducted in New Zealand, Saudi Arabia, the Kyrgyz Republic, Bangladesh, and Malaysia, often employing surveys distributed to target individuals, have revealed a general lack of cybersecurity awareness among both students and the general public. In the UAE, similar studies aimed at assessing the cybersecurity awareness levels among specific groups, such as school teachers and university students, have also demonstrated a significant need for enhanced cybersecurity awareness.

## 2.2 Related Works

### *2.2.1 Cybersecurity Awareness Applications and Games*

In recent years, there has been a significant uptick in the development of mobile and computer games, driven by the global surge in smartphone adoption. This increase in mobile gaming apps, coupled with their strong user engagement, has positioned gaming as a promising avenue for cybersecurity awareness, turning it into a key focus for research [65]. Awareness programs, particularly those employing game-based learning methods, are vital for tackling the challenges of evolving technology. Game-based learning offers

an interactive and enjoyable approach to education, allowing players to develop skills and engage in critical thinking. These games are adaptable and flexible, making them suitable for various training topics. This approach is akin to brain-training apps, effectively enhancing cybersecurity awareness. This paper discusses two mobile games designed to educate users on key cybersecurity aspects: strong password creation and malware protection. "Malware Guardian" focuses on educating users about various security threats, risks, and preventive tools, while "Password Protector" emphasizes the importance of creating, remembering, and regularly updating strong, complex passwords. Both games combine entertainment with practical learning to improve cybersecurity awareness [66].

Researchers in [67] introduced a novel framework to enhance cybersecurity awareness among high school students, focusing on improving password security through gamification. By integrating a serious game into the learning process, the study observed a 5% improvement in students selecting stronger passwords within two months, demonstrating the effectiveness of combining educational content with engaging gameplay to influence secure online behaviors. This approach offers a proof of concept for using narrative and interactive methods to instil cybersecurity principles and indicates potential for broader application and significant impact over longer periods.

A study by [68] aimed to enhance employee cybersecurity awareness through an interactive video game, "Cyber Shield," which embeds various threat scenarios. This game consists of four levels focusing on different aspects of cybersecurity: password complexity, social engineering, phishing attacks, and physical security. The game's effectiveness was evaluated using pre-game and post-game surveys conducted with ten employees from different organizations. The results showed a significant improvement in their cybersecurity awareness, indicating that the Cyber Shield game is more engaging and effective than traditional training methods. The game's interactive nature allows players to simulate responses to cybersecurity threats. The study concludes that such game-based training programs can substantially improve employee cybersecurity awareness and practices.

Researchers in [69] developed a virtual escape room, CySecEscape 2.0, transforming a physical cybersecurity training tool into a digital format to adapt to

constraints like the COVID-19 lockdown to enhance cybersecurity awareness among SME employees. Utilizing the Design Science Research framework, this study created a virtual prototype that addresses cybersecurity challenges SMEs face, such as password hygiene and phishing. The transition to a virtual environment allowed for flexibility in participation, either individually or in pairs, without compromising immersion or educational value. Initial testing with SME representatives and students yielded positive feedback, highlighting the game's effectiveness in conveying cybersecurity concepts through engaging puzzles and scenarios.

A card game called "Riskio" was designed by [70] to enhance cybersecurity awareness among non-technical employees in organizations by simulating attack and defense scenarios in a fictitious company setting. The game encourages active learning by having players alternate roles between attacker and defender, thereby gaining insights into various cyber threats and countermeasures. Riskio aims to create an engaging and interactive learning environment through constructivism learning theory. The evaluation showed that employees found the game more effective in raising cybersecurity awareness compared to students, attributing this to the game's realistic simulation of their work environments. This difference in perception underscores the importance of tailoring cybersecurity education tools to their intended audience.

CybAR is an augmented reality (AR) game designed by [71] to enhance cybersecurity awareness among users, particularly those without a technical background. Developed based on the Technology Threat Avoidance Theory (TTAT), CybAR aims to educate players about various cyber threats and defensive strategies by engaging them in an interactive learning experience. The game, evaluated positively by 91 participants, effectively increases understanding of cybersecurity concepts and demonstrates the practical consequences of cyberattacks, motivating users to adopt safer online behaviors. The main contribution of CybAR lies in its innovative use of AR to create a realistic and engaging learning environment for cybersecurity education, proving to be a fun and effective method for improving players' awareness and knowledge of cybersecurity threats and prevention measures.

"CyberKids" is a serious game application developed by [72] to educate 8 to 12-year-old children on basic cybersecurity concepts, such as strong password use and vulnerability identification, through an engaging and interactive gaming experience. The game, designed with 3D and 2D scenarios, allows children to learn about cybersecurity in a playful yet informative manner. It incorporates gamification techniques to ensure that learning is both fun and effective. The game's design focuses on various cyber threats relevant to children, like social engineering, and uses interactive tasks and feedback to build awareness and skills. The initial validation, although preliminary, suggests that "CyberKids" effectively enhances cybersecurity learning in a playful environment. The main contribution of this study is developing an accessible, engaging educational tool that addresses the increasing need for cybersecurity awareness among young children, encouraging safe online practices from an early age.

A study by [73] explored using gamification to teach average users basic cybersecurity measures, specifically password security, through a role-playing quiz application developed for Android. The application designed using Unity, incorporated RPG elements and multiple-choice questions on password security, rewarding correct answers with points and providing immediate feedback through character health bars. The pilot study with 17 participants revealed that users found the learning experience enjoyable and beneficial, suggesting increased password security knowledge. The main contribution of this research lies in demonstrating the potential of gamified learning to enhance cybersecurity awareness, particularly password security, among average users. The positive response from the study participants indicates that this approach could be expanded to cover more comprehensive security awareness issues, making cybersecurity education more engaging and effective.

Researchers in [74] focused on designing a serious game called Cyber Security-Requirements Awareness Game (CSRAG) to enhance software security awareness. The game aimed to make learning about cybersecurity engaging and effective, integrating concepts like security threats, vulnerabilities, and countermeasures into its gameplay. The methodology involved a literature review to identify research gaps and use this knowledge to design the game. Players participated in a pilot activity by completing pre-questionnaires and suggesting hypothetical scenarios based on real-life cyberattacks. The

results showed that CSRAG positively impacted players' learning outcomes, engagement, and participation, demonstrating that game-based learning is an effective method for teaching cybersecurity scenarios. The main contribution of this research is the development of CSRAG, a tool that effectively combines educational content with an interactive gaming experience, thereby improving cybersecurity awareness and understanding among its players.

A serious game called the Security Requirement Education Game (SREG) was developed by [75] to enhance cybersecurity awareness. The game aims to teach players about security concepts, identify assets and vulnerabilities in organizations, and devise successful security attacks. The game design involved a literature review incorporating cybersecurity knowledge and game-based techniques. SREG proved effective in learning security concepts in a fun and engaging manner and was designed in Chinese and English for wider accessibility. The game emphasizes collaboration within a team while competing with others, taking about 50 minutes to play initially, with time decreasing as players become more familiar with it. Empirical evaluation through observation and a survey indicated that SREG effectively educates players about security attacks and vulnerabilities. Table 7 summarizes the recently proposed games designed to enhance cybersecurity awareness.

Table 7: Recent studies focusing on gamification for cybersecurity awareness

| Reference | Year | Game | Target Audience | Focus / Goal |
|---|---|---|---|---|
| [67] | 2021 | Cyber-Hero | High School Students | Educate students on the importance of password security and avoiding human errors to enhance their protection against cyberattacks. |
| [68] | 2021 | Cyber Shield | Employees | Raise cybersecurity awareness through scenario-based interactive video games. |
| [69] | 2021 | CySecEscape 2.0 | SME employees with basic IT knowledge and advanced IT players | A virtual escape room to raise cybersecurity awareness including physical security, password hygiene, source code security, information disposal, securing sensitive digital data, identity theft and phishing and online banking. |
| [70] | 2020 | Riskio | Employees with no technical background and university students | A tabletop cards game to increase cyber security awareness, specifically on cyber security attacks and defences in an active learning environment |

Table 7: Recent studies focusing on gamification for cybersecurity awareness (Continued)

| Reference | Year | Game | Target Audience | Focus / Goal |
|---|---|---|---|---|
| [71] | 2020 | CybAR | General Audience with no technical background | An AR game to educate users about cybersecurity concepts and show the practical consequences of cyberattacks. |
| [72] | 2020 | CyberKids | Users aged 8 to 12 years | A playful application that integrates and delivers basic educational content on cybersecurity, including games to increase awareness of strong passwords and identify vulnerabilities |
| [73] | 2019 | role-playing quiz app (RPG) | Android Audience | A Unity-based role-playing quiz application for Android, aimed at educating users on password security through targeted questions. |
| [74] | 2019 | CSRAG | General Audience | A card-based game that improves awareness of general security concepts and possible ways to identify threats in the operating environment. |
| [75] | 2018 | SREG | General Audience | Educates players about security requirements based on identified vulnerabilities and security attack scenarios |

Therefore, the exploration of gamification as a tool for enhancing cybersecurity awareness has shown significant promise across diverse demographics and settings. Recent mobile and computer gaming advancements, fueled by a global surge in smartphone adoption, have positioned gamification as a strategic approach for effective cybersecurity education. Through engaging, interactive methods, game-based learning sustains user interest and promotes deeper understanding and retention of cybersecurity concepts. Studies such as those involving "Malware Guardian" and "Password Protector" highlight the practical application of mobile games in educating users about fundamental cybersecurity practices like strong password creation and malware awareness. Similarly, innovative applications like the "Cyber Shield" video game and the virtual escape room "CySecEscape 2.0" demonstrate the adaptability of gamified learning to both individual and organizational contexts, enhancing engagement and efficacy in cybersecurity training. Furthermore, developing games like "Riskio" and "CybAR" emphasizes the role of tailored educational tools that resonate with specific audiences, from non-technical employees to the general public, thereby increasing the accessibility and impact of

cybersecurity education. The positive outcomes observed in these studies—ranging from improved password practices among high school students to enhanced threat recognition in SME employees—underscore the effectiveness of integrating narrative and interactive elements into cybersecurity education.

On the other hand, mobile applications are more capable and usable for lesson-based cybersecurity awareness, and few studies have begun to explore this potential, recognizing the ubiquity and accessibility of mobile devices among individuals. Researchers in [76] explore enhancing cybersecurity behavior through the Theory of Planned Behavior (TPB), augmented with awareness and context-based information factors. A mobile app, CyberAware, was developed to test the proposed model, providing users with targeted cybersecurity news and warnings based on their location, search history, and app usage. After surveying 100 participants, the research validated the model, showing that context-based information significantly boosts users' cybersecurity awareness. The study's key contribution demonstrates that integrating context-based information into cybersecurity education can effectively increase awareness and influence users' intentions and behaviors towards cybersecurity. This approach represents a strategic shift in cybersecurity education, advocating for personalized and relevant information delivery to enhance user engagement and protective behaviors.

The researchers in [77] highlight the increasing concern over cybersecurity threats, particularly among secondary school students in Malaysia, emphasizing the lack of awareness and understanding of cybersecurity among both students and educators. The study, conducted through surveys and interviews with students and counsellors, reveals a significant gap in cybersecurity knowledge and practices among the targeted demographic. The development of the LetSecure mobile application aims to address this gap by offering an educational tool designed to enhance cybersecurity awareness and interest in cybersecurity careers among secondary school students. LetSecure introduces users to various cybersecurity concepts and potential career paths through interactive features such as quizzes and information on cyber threats and prevention methods. The application was developed using the System Development Life Cycle (SDLC) and object-oriented design. The app serves as a beginner-friendly platform for students and others with limited cybersecurity knowledge. The research underscores the crucial need for increased

cybersecurity education and awareness, proposing LetSecure as a valuable resource to mitigate the risks associated with increasing internet usage and foster a safer online environment for young internet users.

A study by [78] presents an innovative educational mobile application to enhance cybersecurity awareness among Arabic-speaking individuals in the MENA region. The application, available on both Android and iOS platforms, incorporates interactive elements such as multiple-choice questions, definitions of key cybersecurity terms, and informative articles. These elements cover crucial topics like social engineering, ransomware, phishing, and secure internet protocols, drawing content from reputable technical sources and incorporating gamification to boost user engagement. The initial release features a comprehensive set of 20 questions, 15 cybersecurity terms, and 30 articles, with plans to expand the content in future updates. The app's main contribution to cybersecurity awareness lies in its focus on the Arabic-speaking population, providing them with vital information on information assurance and cybercrime prevention in their native language. This initiative aims to educate adults and suggests the potential development of a child-friendly version to instill the importance of cybersecurity at a young age. Table 8 summarizes the studies focusing on enhancing cybersecurity awareness through mobile applications based on context information.

Table 8: Mobile application to enhance cybersecurity awareness

| Reference | Year | Mobile App | Target Audience | Focus / Goal |
|---|---|---|---|---|
| [76] | 2021 | CyberAware | Android Audience | Provide users with both effective warnings and relevant cybersecurity information. |
| [77] | 2021 | LetSecure | Secondary School Students | A beginner-friendly educational tool designed to enhance understanding of cybersecurity concepts and encourage interest in cybersecurity careers. |
| [78] | 2020 | Beware of the Hacker "احذر الهاكر" | Adult Arabic-speaking individuals in the MENA region | Enhancing cybersecurity awareness through multiple-choice questions, terms, and articles related to cybersecurity awareness. |

The investigation into mobile applications for enhancing cybersecurity awareness reveals a promising technology integration with educational strategies, addressing specific

needs across various demographics. Mobile apps' unique capabilities to deliver personalized, context-sensitive cybersecurity information make them particularly effective. These applications utilize models such as the Theory of Planned Behavior, augmented with real-time, personalized data such as location and online activity, to significantly elevate user awareness and foster secure online behaviours. Additionally, applications like LetSecure specifically target educational gaps in cybersecurity knowledge among young users, such as secondary school students. By providing interactive learning tools and information about cybersecurity careers, these apps raise awareness and inspire future generations to consider roles in cybersecurity fields. Efforts to develop apps for non-English speaking regions also highlight the importance of cultural and linguistic relevance in cybersecurity education. By providing content in native languages and adapting to local contexts, these applications ensure that essential cybersecurity information is accessible and engaging for a broader audience. Overall, the research conducted demonstrates that mobile applications are an effective tool for enhancing cybersecurity awareness. By leveraging the ubiquitous nature of mobile devices and the potential for tailored educational content, these applications represent a vital component of contemporary cybersecurity education strategies, capable of reaching diverse and widespread audiences.

### *2.2.2 AI in Cybersecurity Education*

The emergence of ChatGPT as a tool for essay writing opens up new possibilities for innovative educational methods. Experts in the field foresee AI technologies like ChatGPT becoming essential in education, proposing integrating technology to enhance learning experiences. One area that can benefit is assessment procedures, as teachers can utilize testing not only as a means of evaluation but also as a tool for learning itself. Moreover, ChatGPT can be leveraged to develop teaching approaches, foster student engagement and collaboration, and promote hands-on, experiential learning. Although ChatGPT is considered disruptive, it presents a significant opportunity to modernize the education system. While some view its ability to generate essays as a potential threat to traditional evaluation methods, it also offers teachers the chance to explore novel approaches for assessing students' knowledge and skills. By incorporating ChatGPT, instructors can enhance evaluation capabilities, encourage student collaboration, and

provide more experiential learning opportunities. ChatGPT is a disruptive technology in education, yet it holds transformative potential through innovative applications [79]. AI technologies such as ML, DL, and NLP can be adapted to deliver personalized and constructive feedback based on user experience and system performance. Also, AI technologies can provide automatic assessments and solutions hints, which enhance the learning process, improve user performance, and support individuals in achieving their goals more effectively.

The Cyber Privacy Advisor Chatbot (CyPACH) was designed by [80] to enhance cyber privacy awareness through interactive training. Utilizing Artificial Intelligence Markup Language (AIML) with platforms like PandoraBot and AndroidJS, CyPACH simulates human-like interactions to educate users on digital privacy and security. The development followed an agile methodology, focusing on digital privacy issues not extensively covered in existing literature. Evaluation through Blackbox testing confirmed the chatbot's functional correctness, while Content Validity assessment, based on expert opinions, verified the relevance and quality of its content, yielding an overall positive validation score of 4.32. This novel approach to cyber privacy education through a chatbot significantly contributes by offering an accessible, engaging method for users to enhance their understanding and practices regarding digital privacy and security.

Researchers in [81] introduced an Automatic Feedback System employing machine learning to provide customized feedback for students on cybersecurity topics. Tested in two undergraduate computer science courses, the system showed promising results: 46% of users reported an enhanced learning experience, 77% expressed interest in further development, and 88% found it effective in teaching basic command-line skills. Despite the positive feedback on command-line skills, the system faced challenges in engaging students with cybersecurity topics, with a notable number of participants struggling to see the connection between command-line usage and cybersecurity. The user interface, inspired by platforms like Codecademy and Khan Academy, was met with average to above-average ratings for user-friendliness. The significant interest in the system's development indicates a demand for such educational tools, highlighting the necessity for more effective integration of cybersecurity topics and accessibility features to cater to a broader range of learners, including those with disabilities.

A Cybersecurity Awareness and Training (CAT) framework was designed by [82] to enhance organizational cybersecurity by evaluating and improving employees' competencies in this domain, particularly during the remote work surge due to the COVID-19 pandemic. This framework, enriched with AI technologies like machine learning and natural language processing, offers a structured approach to cybersecurity education across beginner, intermediate, and advanced levels, comprising 25 core practices. A comprehensive review informed the development of existing models and empirical studies, including insights from cybersecurity professionals. The effectiveness of the CAT framework was validated through case studies in real-world organizational settings, demonstrating its capability to identify employee proficiency levels and guide targeted training to address cybersecurity challenges. The main contribution of this research lies in its innovative use of AI to create a scalable, adaptive framework that supports organizations in systematically enhancing their cybersecurity posture through focused employee education and awareness initiatives.

The Sifu platform, a novel online platform developed by [83] to facilitate CyberSecurity Challenges (CSC) for improving secure coding awareness among software developers, is especially relevant in increasing remote work. The platform uniquely integrates artificial intelligence to automatically assess participants' compliance with secure coding guidelines and provide constructive, solution-guiding hints. This approach supports remote learning and offers a highly interactive and engaging environment for participants to enhance their secure coding practices. Through the deployment of Sifu in real-life CSC events, evaluated via surveys, it was found that the platform significantly contributes to raising awareness about secure coding principles among industry software developers. The platform's architecture allows for the automatic evaluation of code against secure coding guidelines, while its intelligent coach uses AI to lower participants' frustration and guide improvement. The successful application and positive feedback from CSC events underscore the platform's effectiveness in enhancing secure coding awareness, marking a significant contribution to cybersecurity education by leveraging AI to offer an adaptive, engaging learning experience. Table 9 summarises the studies that illustrate the use of AI in enhancing cybersecurity awareness and advancing cybersecurity education.

Table 9: AI in enhancing cybersecurity awareness

| Reference | Year | Main Contribution | Description |
|---|---|---|---|
| [80] | 2023 | A chatbot powered by Artificial Intelligence Scripting Language implemented by PandoraBot and AndroidJS to mimic human communications. | Developed to act as a Cyber Privacy Advisor, serving as a training tool for individuals seeking to attain a proper level of awareness regarding cyber privacy. |
| [81] | 2022 | Automatic Feedback System based on Machine Learning to Teach Cybersecurity Principles to K-12 and College Students | Deliver personalized and constructive feedback on cybersecurity topics tailored to individual users based on user experience and system performance. |
| [82] | 2022 | Cybersecurity awareness and training (CAT) framework-based AI, specifically ML and NLP to provide a self-adaptive and smart framework designed for employees. | Provide customized training for employees and increase awareness of recent social-engineering-based cyber-attacks and threats. |
| [83] | 2020 | (Sifu) cybersecurity awareness platform that uses AI to provide players with solution-guiding hints (intelligent hint generation) and automatic cybersecurity challenge assessment. | Raise awareness on secure coding, secure coding guidelines, and software development best practices |

Incorporating AI in cybersecurity awareness and education marks a significant evolution in teaching methods, providing more personalized, engaging, and effective learning experiences. Tools like ChatGPT and other AI technologies, including ML and NLP, have opened new avenues for enhancing educational content delivery and engagement. These technologies enable the development of platforms that offer customized feedback, adaptive learning paths, and interactive experiences, which are crucial for effective cybersecurity education. AI's capability to simulate real-life interactions and provide real-time, context-aware feedback helps make learning more relatable and impactful for users. This approach improves the learner's engagement and enhances their ability to apply cybersecurity knowledge practically. The use of AI in educational tools has shown potential in various settings, from individual learning apps to organizational training frameworks, reflecting its adaptability and scalability. By leveraging AI, educational platforms can significantly enrich the learning experience, making complex cybersecurity concepts more accessible and understandable. As AI

technologies continue to advance, their integration into cybersecurity education promises to further empower learners and educators, driving the development of more secure digital environments.

Therefore, there is a compelling need for innovative approaches in cybersecurity education, particularly through mobile applications and the integration of AI technologies. While research has underscored a general lack of cybersecurity awareness globally, studies in the UAE have also indicated a significant gap in awareness among key demographic groups such as school teachers and university students. This gap highlights the urgent need for targeted educational tools within the UAE. Gamification and mobile applications have effectively enhanced cybersecurity awareness across diverse demographics. These methods maintain user engagement and foster a deeper understanding of cybersecurity practices through interactive and context-sensitive learning experiences. Mobile applications like LetSecure, tailored to address educational gaps among the youth, and AI-driven tools such as ChatGPT, which offer personalized learning enhancements, illustrate the successful application of these technologies in improving cybersecurity awareness. However, there is a notable scarcity of such studies and applications, specifically within the UAE, signalling a significant opportunity to develop localized mobile applications. These applications could utilize AI to enrich the learning experience by adapting content to the cultural and linguistic context of the UAE, ensuring greater relevance and engagement. Introducing a mobile application designed for UAE individuals could leverage AI to enhance user engagement effectively. By providing real-time, personalized feedback and adaptive learning paths, such a tool could significantly improve UAE residents' cybersecurity behaviour and awareness. This application could include features such as scenario-based learning modules, interactive quizzes, and gamified elements, all tailored to the unique cybersecurity threats individuals in the UAE face. Incorporating AI promises to make learning about cybersecurity more accessible and engaging and ensures that the educational content is deeply embedded with the latest practices and recommendations tailored to real-world applications. As AI technologies continue to evolve, their potential to transform cybersecurity education into a more interactive, engaging, and effective discipline is immense. In conclusion, the limited studies and applications in the UAE and the proven effectiveness of mobile applications and AI in

enhancing cybersecurity awareness strongly advocate developing a localized educational tool. Such a tool could significantly contribute to the national cybersecurity posture by elevating individual awareness and defence capabilities, preparing citizens and residents to face evolving cyber threats.

# Chapter 3: Research Methodology

The chapter outlines the research design and approach to address the challenges identified in the literature review and the objectives of enhancing cybersecurity awareness in the UAE by developing an AI-enhanced mobile application. This chapter provides a detailed explanation of the methods employed for data collection, analysis, and the development process of the mobile application. It begins with a research framework containing five phases that justify the chosen research methodology, whether qualitative, quantitative, or mixed-methods approach, and discusses the rationale behind selecting tools, techniques, and procedures. The chapter delineates the processes involved in assessing the current state of cybersecurity awareness, identifying educational gaps, and exploring the integration of AI technologies. It also describes the AI-enhanced mobile application's design, development, and evaluation stages.

## 3.1 Research Framework

Cybersecurity education and awareness are paramount in the digital era due to the field's continuous evolution and rapid adaptation. Figure 3 presents a comprehensive research framework designed to evaluate and enhance cybersecurity awareness. This framework is structured into five distinct phases, each serving as a foundational pillar for developing an integrated solution. The proposed framework provides a theoretical and practical guide that culminates in developing a mobile application tailored to the identified educational needs. For clarity and coherence, each phase is compartmentalized into specific, actionable steps that sequentially build upon one another.

This systematic approach ensures coverage across a broad spectrum of age groups within the UAE community. In Phase 1, we concentrate on pinpointing the limitations and gaps within the cybersecurity curricula of schools and universities cybersecurity programs, as well as the challenges students may face. Phase 2 comprises a study aimed at gauging the level of cybersecurity awareness and the implementation of best practices among UAE residents aged 18 and above. Phase 3 will present the synthesis of these findings and steer the development of targeted solutions, which materialize through phase 4, the development of a mobile application. The thesis concludes with an evaluation of the impact of these interventions and the acknowledgement of any remaining limitations,

setting the stage for future research and development in the domain of cybersecurity education and awareness.

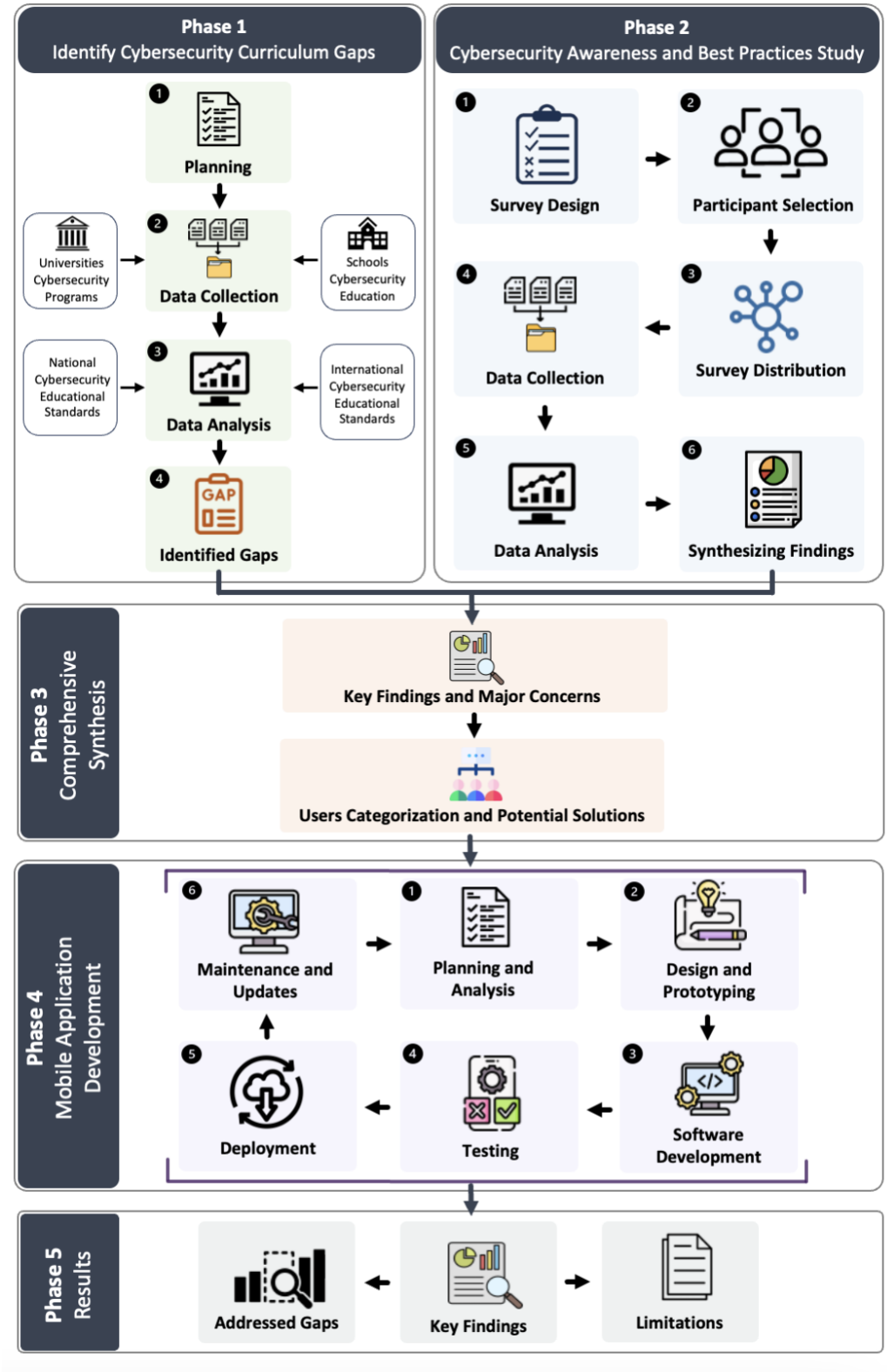



Figure 3: Research Framework

### 3.2 Phase 1: Identify Cybersecurity Education and Curriculum Gaps

This phase aims to comprehend the foundational knowledge of cybersecurity by examining the structure and content of cybersecurity curricula in educational institutions, teaching methodologies, and adherence to academic standards. The objective is to identify any gaps in cybersecurity knowledge, skills, or best practices and to illustrate the impact of these gaps on student preparedness.

#### *3.2.1 Plaining*

The main focus of this phase will be exclusively on schools following the Ministry of Education (MoE) curricula and universities offering cybersecurity or information security programs in the UAE. This deliberate concentration on these educational institutions allows for a detailed analysis of existing curricula, enabling us to identify specific areas where enhancements are needed in terms of cybersecurity awareness. The planning will involve a thorough review of the MoE's curriculum guidelines and an examination of the learning outcomes within higher education cybersecurity programs. This selection ensures a comprehensive understanding of the current state of cybersecurity education at both the school and university levels within the UAE.

#### *3.2.2 Data Collection*

In the data collection, we will systematically revisit the cybersecurity curricula across the UAE to pinpoint existing gaps. This will involve collecting materials from the MoE's curricula for school students in grades 1 through 12. For universities, our approach will include assessing the number of institutions offering security-related programs within the UAE and conducting a detailed review of the learning outcomes for each program.

#### *3.2.3 Data Analysis*

The data analysis phase will thoroughly compare the collected data with national and international cybersecurity education standards and best practices. This comparison aims to identify areas requiring enhancement, such as foundational knowledge, advanced skills, and the latest best practices in emerging cybersecurity fields. Furthermore, the analysis will explore the implications of these findings for graduate readiness and

workforce development, specifically examining how these gaps affect student preparedness for cybersecurity threats and challenges.

### *3.2.4 Identified Gaps*

We will focus on identifying gaps that can be effectively addressed by developing a mobile application, including underrepresented cybersecurity awareness-related domains, educational voids, essential skills, and cutting-edge practices.

## 3.3 Phase 2: Cybersecurity Awareness and Best Practices in the UAE

This phase aims to enhance our understanding of cybersecurity awareness among individuals in the UAE through the deployment of a survey. This survey specifically addresses the existing gap in the literature regarding empirical data on cybersecurity awareness in the region. Given the absence of recent studies providing statistics on cybersecurity awareness among UAE individuals, this survey is crucial to identify where weaknesses or discrepancies lie in the knowledge, skills, and implementation of best practices in cybersecurity. The objective is to conduct a detailed statistical analysis that clarifies these areas, enabling targeted improvements in cybersecurity education and practices.

### *3.3.1 Survey Design*

The survey design for cybersecurity awareness and best practices in the UAE is carefully crafted to comprehensively understand individuals' knowledge, attitudes, and behaviors regarding cybersecurity. This design encompasses a range of questions that cover demographic information, general awareness of cybersecurity concepts, personal practices and experiences related to cybersecurity, and preferences for learning about cybersecurity. The questions are structured to elicit both quantitative and qualitative responses, allowing for a nuanced analysis of cybersecurity awareness among diverse population segments in the UAE.

### *3.3.2 Participation Selection*

Participants for this survey are selected to represent a wide cross-section of the UAE's population, including age groups above 18, educational backgrounds, employment

statuses, and regions within the country. The selection process aims to ensure a diverse and representative sample that can provide insights into cybersecurity awareness and practices across various demographic and social groups in the UAE.

### *3.3.3 Survey Distribution*

The survey was designed to be distributed in both Arabic and English to accommodate the linguistic diversity of the UAE's population. Google Forms was selected for its accessibility and ease of use; the survey was disseminated randomly to potential participants through various channels, including social media, educational institutions, and professional networks. This approach is designed to maximize participation rates and ensure the broad reach of the survey.

### *3.3.4 Data Collection*

Data collection through the survey focuses on gathering detailed responses to questions related to cybersecurity awareness, experiences with cyber threats, and preferences for cybersecurity education. The anonymity and confidentiality of participants' responses are prioritized to encourage honest and accurate feedback. Google Forms facilitates efficient data collection and management, allowing for real-time monitoring of response rates and participant engagement.

### *3.3.5 Data Analysis*

After the data collection phase is completed, the responses will be analyzed to identify trends, patterns, and gaps in cybersecurity awareness and practices among the participants. Quantitative data will be subjected to statistical analysis to measure the prevalence of various awareness levels and practices, while qualitative responses will be analyzed for thematic content to gain deeper insights into participants' perceptions and experiences.

### *3.3.6 Synthesizing Findings*

The final step involves synthesizing the findings from the survey data to conclude the state of cybersecurity awareness and best practices in the UAE. This synthesis will highlight key areas of strength and identify weaknesses or critical gaps in knowledge and

practices concerning cybersecurity awareness that can be addressed by developing a mobile application.

### 3.4 Phase 3: Comprehensive Synthesis

This phase serves as the integrative core of the research, where we consolidate the crucial findings and principal concerns surrounding cybersecurity awareness from Phase 1 (Identifying Cybersecurity Curriculum Gaps) and Phase 2 (Cybersecurity Awareness and Best Practices Study in the UAE). This phase aims to distill the collected data into actionable insights, outlining the potential solutions that will be realized through developing a mobile application in Phase 4. A key component of this synthesis is the categorization of users based on their unique needs and vulnerabilities as identified through the earlier phases. This user-focused analysis is crucial for developing the mobile application to bridge the cybersecurity knowledge gaps effectively across different user categories in the UAE.

### 3.5 Phase 4: Mobile Application Development

This phase will be meticulously constructed based on the findings and insights gathered from the previous phases, ensuring that the development of the mobile application is data-driven and centred around the user experience. The development of the mobile application will adhere to the software development life cycle (SDLC), with each step, from planning and analysis through to maintenance and updates, being integral and interconnected in the creation of an application that effectively enhances cybersecurity awareness among users. The primary focus of this phase is to deliver an educational tool tailored to the specific cybersecurity needs identified within the context of the UAE.

#### *3.5.1 Planning and Analysis*

This stage of mobile application development sets the strategic direction for the development. In this phase, we will define the mobile application's scope, objectives, and specifications, guided by the insights gathered from the previous phases. This involves understanding the user needs, the educational gaps identified in the curriculum, and the specific areas of cybersecurity awareness that require attention.

### *3.5.2 Design and Prototyping*

Following the initial planning, the design and prototyping phase focuses on creating the application's user interface and experience (UI/UX) by drafting layout sketches, wireframes, and interactive prototypes to visualize the app's functionality and aesthetics. This phase is iterative, involving continuous feedback and editing to ensure the application is both intuitive and engaging, which will also bridge the application's conceptual design and actual development.

### *3.5.3 Software Development*

Software development is the execution phase where the actual coding of the application takes place. Utilizing the React Native framework, we aim to create a cross-platform solution that ensures a consistent user experience across iOS and Android devices. For secure user sign-in and registration, we will integrate Firebase Authentication to manage user identities reliably. Firebase authentication will be combined to secure user authentication, providing reliable identity management. The application's back end will be powered by Firebase Cloud Firestore, enabling real-time synchronization of text-based data, and Firebase Cloud Storage will provide scalable cloud-based storage for multimedia content.

### *3.5.4 Testing*

Testing is an exhaustive phase where every aspect of the mobile application undergoes rigorous scrutiny to ensure technical and educational efficacy. This includes automated and manual tests to identify and rectify issues, such as unit, integration, system, and user acceptance. The testing phase validates the application's performance, security, and usability across various devices and user scenarios, ensuring that the application is reliable and ready for deployment.

### *3.5.5 Deployment*

The deployment marks the launch of the mobile application to end-users. This involves setting up the production environment, finalizing the app's release version, and submitting it to app stores for distribution. The deployment process will be carefully

managed to ensure a smooth launch, enabling users to download and install the application easily.

### *3.5.6 Maintenance and Updates*

The maintenance and update phase is critical for the application's longevity and relevance post-deployment. Continuous monitoring of the application's performance is conducted, with regular updates to address any emerging issues and improve features. This phase ensures that the mobile application remains a current and effective tool for cybersecurity awareness, providing users with the most up-to-date information and learning resources.

## 3.6 Phase 5: Research Results

Finally, this phase will present the main results of our findings, thoroughly detailing how the mobile application has effectively addressed the gaps in cybersecurity awareness identified in the initial phases of the research. This phase will outline the key findings, showcasing the application's impact on enhancing cybersecurity awareness and practices among its users. It will also explore the limitations encountered during the application's development and implementation.

# Chapter 4: Cybersecurity Education Gap Identification in the UAE

This chapter is dedicated to uncovering the gaps in cybersecurity awareness within the educational curricula of schools and universities in the UAE. Initially, our attention will be directed towards examining the present condition of cybersecurity education in public and private schools that follow the MoE curriculums. A specific emphasis will be placed on the Computing Creative Design Innovation (CCDI) subject, where we aim to dissect the cybersecurity context integrated within this subject to pinpoint existing gaps in cybersecurity awareness. Subsequently, we will delve into higher education by evaluating universities that offer cybersecurity-related programs. Here, our focus will shift to identifying gaps in the learning outcomes of these programs, especially concerning imparting cybersecurity knowledge, fostering awareness, enhancing skills, and preparing students for the cybersecurity workforce.

## 4.1 Curriculum Gap Identification in the Public Schools in the UAE

### *4.1.1 Current State of Cybersecurity Education*

The MoE in the UAE, established following the country's formation in 1971, plays a pivotal role in shaping the educational landscape across all emirates. Tasked with developing a national curriculum that integrates a wide spectrum of subjects while embedding the UAE's values and culture, the MoE's efforts extend to both public and select private schools. With a vision to pioneer innovative education for a knowledgeable and globally competitive society, the MoE sets forth a mission to cultivate an education system that spans all age groups, aligning with future labour market demands through quality outputs. Strategic objectives focus on inclusive education, leadership, educational efficiency, and fostering an environment ripe for scientific research and innovation. The Ministry's commitment to leveraging advanced technologies, alongside continuous curriculum enhancement, aims to equip students with the skills needed for the 21st century, driving forward the nation's agenda for creativity, innovation, and global competitiveness [84], [85].

The MoE has designed a structured K-12 education system for government schools, starting with a two-level kindergarten for 4 to 5-year-olds that lays the foundation for

primary education and beyond. In 2018, the Ministry restructured school cycles to include four grades per stage, streamlining the path from primary through secondary education. Primary education, or Cycle 1, covers Grades 1 to 4, fostering a vibrant learning atmosphere for young learners. The intermediate level, or Cycle 2, from Grades 6 to 8, focuses on developing students into well-rounded individuals, while the secondary level, or Cycle 3, from Grades 9 to 12, prepares students for their future careers and societal roles, culminating in a high school certificate. The educational streams have evolved from a binary choice between scientific and literary paths to four distinct streams: general, professional, advanced, and elite (Advanced Science Program-ASP), offering students tailored learning paths based on their performance and interests, from practical vocational training in the professional stream to intensive math and science focus in the advanced and elite streams, ensuring a comprehensive education that caters to diverse student needs and aspirations [86].

The MoE organizes the academic year into three terms, offering a structured curriculum divided into two main categories to cater to the diverse learning needs of students. Within this framework, Category B is specifically designed to enhance the educational experience by incorporating subjects that align with students' skills, age, and academic levels. One of the subjects in Category B is CCDI [87]. The CCDI curriculum aims to forge students equipped with a blend of computing, creativity, innovation, and problem-solving skills prepared for the complexities of the modern world. This initiative reflects a strategic commitment to fostering entrepreneurial abilities and a deep understanding across design, engineering, and computer science, emphasizing STREAM education (Science, Technology, Reading, Engineering, Art, Maths and AI) to enable students to excel in a globally competitive environment. CCDI curriculum is structured around five key domains to ensure a well-rounded education that spans computer science, engineering, design and innovation, with a focus on sustainability and visual communication, thus equipping students with the essential skills for future challenges and opportunities [88].

The CCDI curriculum incorporates various tools and resources to enhance students' networking and cybersecurity abilities and skills [88]. In Cycle 1, encompassing grades 1 to 4, during the first term, the CCDI curriculum textbooks introduces several learning

outcomes about the basics of computer systems. Specifically, in Unit 1 of the Grade 3 CCDI curriculum textbook, the primary learning outcomes include identifying the fundamental components of a computer system, solving basic problems related to computer hardware and software, and understanding simple troubleshooting strategies. Students will develop key skills and an understanding of computing technologies, including computer systems, processes, and hardware and software problems. Students will have few simple activities related to computing technologies, such as searching for keywords, matching computer elements and computer systems, distinguishing common hardware and software problems, and ending the unit with a short quiz [89], [90]. Meanwhile, Unit 1 of the Grade 4 CCDI curriculum textbook expands on these topics by adding additional learning outcomes. These include demonstrating how various devices and components interact, analyzing the functions of computer hardware and software within a system, assessing the significance of each system component, offering solutions to common hardware and software issues, and explaining the flow of information packets across the internet. To aid in understanding these concepts, students are provided with diverse examples, engaging activities, and quizzes related to the subject matter. Activities range from keyword searches and True/False statements to matching hardware and software names and identifying key components of computer systems [91], [92]. Notably, the curriculum for grades 1 and 2 does not contain any networking or computer security-related material within their CCDI workbooks/coursebooks [93]-[96]. In Term 2, the CCDI curriculum textbooks for Cycle 1 cover the following topics: Grades 1 and 2 focus on 2D/3D shapes and visuals, robots, sensors and intelligent devices, and entrepreneurship [97], [98]. Grades 3 and 4 delve into motion and force, robotics, algorithms, programming and interfaces, design, embedded systems and microcontrollers, and electric circuits [99], [100]. Both terms conclude with STREAM projects for all grades. Therefore, Term 2 of the CCDI curriculum for Cycle 1 does not include any content related to cybersecurity.

In Cycle 2, covering grades 5 to 8, the first term of the CCDI curriculum textbooks introduces learning outcomes across a range of topics, including embedded systems, algorithms and programming, data analysis, networks and the internet, culminating in an end-of-term project. This project requires students to analyze hardware and software issues and assess potential solutions. Each unit across the grades begins with e-safety topics,

which cover the following topics: identity theft, the creation of strong passwords, online privacy, cyberbullying, the impact of computing on mental health, distinguishing between public and private information, the effects of computing technologies, technology biases, and the UAE positive digital citizenship character. These topics are presented in a concise and simplified manner, spanning only one or two pages at the beginning of each unit [101]-[108]. In the second term for grades within Cycle 2, the content structure mirrors that of the first term, with each grade exploring four units. These units encompass topics such as computer and embedded systems, an introduction to robotics, electricity and electronics, robotics and systems in action, the engineering design process and its impacts, a sustainable society and technical graphics, culminating in an end-of-term project. Each unit begins with an e-safety introductory topic, offering tips and advice; some of these e-safety topics revisit themes from Term 1. The e-safety topics for this term include protecting yourself on the internet, maintaining a safe class workspace, reducing computer waste, understanding cybercrimes, social media addiction, adhering to information ethics, software privacy, digital citizenship, e-safety guidelines, and differentiating between public and private information with theoretical, interactive, and lab activities for each unit [109]-[116].

Cycle 3, encompassing grades 9 to 12, focuses on advanced topics in the CCDI curriculum. In the second term, Grade 9 students are introduced to four chapters: electricity and electronics, graphics for design, principles of computer-aided design, and design realization, with each chapter further divided into two sections. Grade 10 students in the general CCDI curriculum explore themes such as sustainable society, graphics for design, and 3D design realization. For both grades 9 and 10, a series of activities is provided to enhance the knowledge and skills acquired [117]-[120]. Accordingly, the curriculum for these levels in Term 2 does not include any content related to cybersecurity. Conversely, students in grades 11 and 12 follow the elective model of the MoE curriculum, which entails taking six compulsory subjects and having the option to choose elective subjects. Within this framework, the CCDI subject is categorized as an elective, providing students with the flexibility to decide whether to include it in their academic journey [121]. The general CCDI curriculum for grades 11 and 12 in Term 2 is centered around topics such as the fundamentals of electronic circuits, 3D design realization, AI, methods of achieving

AI, and the future of AI [122]-[125]. Neither level includes content related to cybersecurity. Meanwhile, the advanced CCDI curriculum for grades 11 and 12 delves into topics like the software life cycle, the basics of operating systems, the Internet of Things (IoT), and AI [126]-[129]. Across all grades, a project and variety of activities are incorporated, all adhering to a STREAM approach.

In summary, Cycle 1, during Term 1 of the CCDI curriculums, introduces basic information about computer systems. Cycle 2 addresses key e-safety topics in both Term 1 and Term 2. Cycle 3, in Term 2, explores a range of advanced topics; however, it does not include content related to cybersecurity.

### *4.1.2 Identified Gaps and Their Implications*

The absence of direct cybersecurity content in early education (Cycle 1) is notable. The curriculum for grades 1 to 4 is primarily centered on basic computing skills, with a glaring omission of direct cybersecurity concepts. This lack of inclusion misses a crucial opportunity to instill foundational cybersecurity awareness at an early age. Consequently, the absence of cybersecurity education in the initial schooling years can result in a fundamental gap in understanding and awareness of online safety and security risks among younger students.

While e-safety topics are introduced in middle school (Cycle 2), there is a noticeable lack of in-depth cybersecurity education for grades 5 to 8. The curriculum mainly emphasizes broader computing concepts and digital citizenship without adequately covering the principles and practices of cybersecurity. This restrained incorporation of cybersecurity topics into the middle school curriculum overlooks vital opportunities to cultivate skills crucial for identifying and mitigating cyber threats, which are becoming increasingly significant in students' digital lives.

The absence of cybersecurity education in high school (Cycle 3) is noticeable. In grades 9 to 12, despite including advanced computing topics such as AI and the Internet of Things, the curriculum lacks explicit instruction on cybersecurity. This omission fails to address the essential requirement of arming students with the necessary knowledge to defend against cyber threats. The lack of dedicated cybersecurity education in these higher

grades leaves students potentially ill-equipped to deal with the sophisticated nature of modern cyber threats. Furthermore, allowing CCDI to be an elective subject in grades 11 and 12 permits students to bypass this critical area of education, potentially resulting in a knowledge gap for those who could significantly benefit from this subject.

This section's analysis was confined to the CCDI curriculum materials for Terms 1 and 2, and it did not encompass the content for Term 3 or the materials for grades 9 to 12 in Term 1. This limitation in scope means that the overview provided here may not fully represent the entirety of the CCDI curriculum, particularly in the areas not reviewed.

## 4.2 Gap Identification in Universities Cybersecurity Programs in the UAE

### *4.2.1 Overview of Current Cybersecurity Programs*

According to the MoE and the Commission for Academic Accreditation (CAA), there are 74 active higher education institutions in the UAE. Among these, 18 universities offer cybersecurity-related programs, which represents approximately 24% of all universities in the UAE. Out of the 1,285 accredited active programs in the UAE, there are 27 programs (higher diplomas, bachelor's degrees, and master's degrees) related to cybersecurity [130], [131]. Table 10 lists the universities and their respective cybersecurity programs.

Abu Dhabi Polytechnic's Information Security Engineering Technology (ISET) program is designed to develop skilled engineers and technologists in cybersecurity, adhering to international standards. The program focuses on the critical aspects of securing infrastructure, offering comprehensive learning outcomes that include the ability to protect assets, strategize for cybersecurity, and design secure systems. It also covers the ethical and legal dimensions of the field. Graduates will possess a wide-ranging understanding of information security technologies and be prepared for system development, networking, and administration roles, with a commitment to ongoing professional development. The program grants a higher diploma and an applied bachelor's degree [132]

Abu Dhabi University excels in cybersecurity education with its Bachelor of Science in Cybersecurity Engineering and Information Technology with a Cybersecurity Concentration. Tailored to support the Abu Dhabi Vision 2030, these programs aim to

prepare graduates for the evolving tech market. The learning outcomes ensure graduates can apply computing, engineering, and mathematics knowledge to identify solutions to cybersecurity challenges, design secure systems that meet specific requirements, and effectively communicate in professional settings. Additionally, the curriculum prepares students to approach cybersecurity responsibilities with ethical and legal integrity, work collaboratively in multidisciplinary teams, and maintain a commitment to lifelong learning to adapt to the rapidly changing technology landscape [133].

Ajman University offers a Bachelor of Science in Information Technology with a Concentration in Networking and Security to prepare students for the dynamic field of information technology and cybersecurity. The program aims to provide high-quality education that meets international standards to create IT professionals adept at addressing market and societal needs. The program objectives include preparing graduates for successful careers in the IT sector, enabling them to tackle technical, business, or ethical challenges in information technology, and encouraging lifelong learning. The curriculum covers analyzing computing issues, implementing solutions, effective communication, moral responsibility, and applying security measures against threats [134].

Al Ain University's Bachelor of Science in Cybersecurity is designed to meet the UAE and Gulf region's cybersecurity demands. The program's learning outcomes are structured to ensure graduates can analyze complex computing issues, design and implement sustainable computing-based solutions, and effectively communicate within professional contexts. Additionally, graduates will have a keen awareness of their professional responsibilities, the ability to make informed decisions based on legal and ethical principles, and the ability to function effectively in team settings. This curriculum equips students with the necessary skills for various job roles in the cybersecurity sector, such as analyst, engineer, and consultant roles, supporting the UAE's national cybersecurity goals and meeting the demand for skilled IT professionals [135].

The American University in the Emirates offers specialized programs in cybersecurity, including a Bachelor of Science in computer science with concentrations in digital forensics and network security, and a master’s in security studies and information analysis. These programs aim to prepare students for the IT industry's demands by

providing them with the necessary skills to address complex computing problems, implement security solutions, and conduct applied research in cybersecurity. Graduates are expected to analyze and design computing-based solutions, communicate effectively, and apply critical thinking in professional and ethical decision-making. Tailored to support the UAE's Vision 2030, these programs cater to the regional need for skilled cybersecurity professionals and information analysts [136], [137].

Amity University Dubai provides a Bachelor of Science in Computer Science with a Cybersecurity concentration, preparing students with broad knowledge in key areas such as software design, machine learning, and cybersecurity. The program enhances research skills and understanding of technological innovation through advanced labs, preparing students for IT careers or roles in diverse sectors. The curriculum emphasizes problem-solving with mathematical and engineering principles, preparing graduates for various IT-related careers. Learning outcomes include problem analysis, solution design, effective communication, ethical professional practice, teamwork, and applying core computer science concepts. Cybersecurity concentration graduates gain specialized skills in network security analysis, cybersecurity policy formulation, and IT infrastructure protection [138].

The British University in Dubai provides a Bachelor of Science in Computer Science with a Cybersecurity concentration and a Master of Science in Cybersecurity, aimed at preparing students to tackle cyber threats effectively. The undergraduate program develops skills in system security, AI technologies for cybersecurity, and software engineering best practices, preparing students for roles such as security consultants and cyber forensics experts. The postgraduate program offers a comprehensive overview of cybersecurity, from governance to digital forensics. It aims to produce skilled professionals capable of designing, defending, and managing secure systems in diverse sectors. Learning outcomes for both programs include the ability to analyze computing problems, design and evaluate solutions, apply cybersecurity knowledge innovatively, and understand professional responsibilities within legal and ethical frameworks [139], [140].

Canadian University Dubai's Bachelor of Science in Cyber Security prepares students for the network security industry with a curriculum that spans computer systems, forensics, ethical hacking, and applied cryptography. Emphasizing theory and practical

skills, the program aims to produce graduates capable of addressing cyber threats and contributing to the UAE's Smart City initiatives. Graduates are equipped for roles such as Chief Information Security Officer (CISO), Forensic Computer Analyst, and Penetration Tester [141].

The Higher Colleges of Technology provide a Bachelor of Information Technology with a Security and Forensics concentration aimed at preparing skilled IT professionals proficient in solving complex problems with ethical approaches. This program offers a solid technical foundation, professional competencies, and specialized knowledge in security and forensics, among other IT areas. Graduates will be equipped to develop and manage secure networking technologies, apply security practices against risks, and effectively work in teams. This comprehensive education ensures readiness for the IT industry, emphasizing lifelong learning and professional development [142].

Khalifa University offers a Bachelor of Science in Computer Science with a Concentration in Cybersecurity and a Master of Science in Cyber Security. The undergraduate program focuses on theoretical foundations and practical applications in computing and cybersecurity, including AI/ML, applied cryptography, and digital forensics. Graduates are expected to develop, implement, and evaluate computing solutions, communicate effectively, and undertake leadership roles while adhering to ethical standards. The master's program deepens knowledge in cybersecurity, emphasizing research, problem-solving with modern tools, knowledge integration, experiment design, and ethical professional conduct. Graduates of both programs are prepared for diverse careers in software development, security management, ethical hacking, and more across various industries, including ICT, government, finance, and healthcare [143], [144].

Rochester Institute of Technology-Dubai offers a Bachelor of Science and a Master of Science in Computing Security, preparing students for a range of careers in cybersecurity. The curriculum covers various topics, including computer systems, network and computer forensics, ethical hacking, and applied cryptography, alongside hands-on and theoretical learning. Graduates are equipped to address cybersecurity vulnerabilities, implement security solutions, and take on roles such as cybersecurity analysts, engineers,

and consultants. The program emphasizes developing skills for lifelong learning, teamwork, leadership, and ethical practice in cybersecurity [145], [146].

UAE University offers a Bachelor of Science and a Master of Science in Information Security, designed to equip students with the necessary management skills and technical knowledge for information and network security operations. The undergraduate program focuses on applying proven and innovative practices for securing systems, applications, and networks, meeting the need for IT specialists skilled in information security. Graduates are expected to analyze complex computing problems, design and evaluate computing-based solutions, communicate effectively, and apply security principles in various professional contexts. The graduate program aims to develop expertise in information security leadership and operations, providing the technical and managerial skills necessary to secure IT architectures and formulate information security policies. Both programs emphasize ethical practice, lifelong learning, and compliance with international standards and local policies, preparing students for professional roles in information security and further academic pursuits [147], [148].

The University of Dubai's Master of Science in Cyber Security program equips graduates with advanced knowledge and skills in cybersecurity to address cybersecurity risks, employ modern tools for threat handling, and enhance security measures in digital environments. It also prepares participants for a wide array of cybersecurity roles in the public and private sectors, catering to the increasing demand for experts capable of protecting against evolving cyber threats [149].

The University of Fujairah offers a Bachelor of Information Technology with a specialization in Networking and Security, aimed at equipping students with the necessary skills to develop, manage, and secure computer networks and information systems. This program focuses on practical solutions to networking and security challenges, emphasizing ethical practices, innovative solutions, and effective communication. Graduates are prepared for various roles, such as cybersecurity analysts and digital forensic examiners [150].

The University of Science and Technology of Fujairah offers a Bachelor of Science in Information Technology specializing in Cyber Security, aiming to produce skilled

cybersecurity professionals. Graduates are expected to apply their knowledge and skills across the public and private sectors, demonstrate leadership in technical and ethical realms, and engage in lifelong learning and research. The program prepares students and graduates for diverse roles such as security analyst and security software developer, emphasizing lifelong learning, research, and the application of IT solutions within the UAE and Gulf region [151].

The University of Sharjah's Cybersecurity Engineering programs at both Bachelor and Master levels aim to develop skilled professionals ready to tackle cybersecurity challenges and are designed to address the increasing demand for qualified cybersecurity professionals by providing comprehensive education on protecting computer systems from cyberattacks. Students will explore various aspects of cybersecurity engineering, including secured computer architecture, digital forensics, cryptography, and data hiding. The curriculum includes both theoretical and practical training, preparing graduates for careers such as IT security engineers, network security engineers, and cybersecurity architects. Graduates will have the skills to solve complex cybersecurity problems, apply engineering design considering societal needs, communicate effectively, understand professional responsibilities in cybersecurity contexts, and use advanced engineering tools for data analysis and research [152], [153].

The University of Wollongong in Dubai offers a Bachelor of Computer Science with a specialization in Cyber Security, focusing on equipping students to tackle the complexities of information security in today's technology-driven world. This program addresses the urgent need for experts who can secure information systems against emerging cyber threats, especially with the proliferation of the IoT. Graduates are prepared for careers such as information security analyst, CISO, security architect, and ethical hacker, fulfilling the global demand for cybersecurity professionals [154].

Zayed University offers a Bachelor of Science in Information Technology with a Concentration in Security and Network Technologies and a Master of Science in Information Technology with a Concentration in Cyber Security. The undergraduate program develops skills to secure information systems and design secure networks, while the graduate program focuses on network security, database security, digital forensics, and

ethical hacking. Graduates are equipped for roles such as security analysts, cyber security specialists, and digital forensic analysts to address cybersecurity challenges in various sectors. The curriculum combines theoretical knowledge with practical laboratory experiences, offering options for thesis and non-thesis tracks to cater to individual career aspirations [155], [156].

Table 10: ACC-Accredited Active Cybersecurity-Related Programs in the UAE

| **University** | **Program** |
|---|---|
| Abu Dhabi Polytechnic | Higher Diploma/Applied Bachelor in Information Security Engineering Technology<br>Concentrations: Network and Cyber Security, Software Security, Systems/Servers Security Administration |
| Abu Dhabi University | Bachelor of Science in Cybersecurity Engineering |
| | Bachelor of Science in Information Technology<br>Concentration: Cybersecurity |
| Ajman University | Bachelor of Science in Information Technology<br>Concentration: Networking and Security |
| Al Ain University | Bachelor of Science in Cybersecurity |
| American University in The Emirates | Bachelor of Science in Computer Science<br>Concentrations: Digital Forensics, Network Security |
| | Master in Security Studies and Information Analysis |
| Amity University Dubai | Bachelor of Science in Computer Science<br>Concentration: Cybersecurity |
| British University in Dubai | Bachelor of Science in Computer Science<br>Concentration: Cyber Security |
| | Master of Science in Cyber Security |
| Canadian University Dubai | Bachelor of Science in Cyber Security |
| Higher Colleges of Technology | Bachelor of Information Technology<br>Concentration: Security and Forensics |
| Khalifa University | Bachelor of Science in Computer Science<br>Concentration: Cybersecurity |
| | Master of Science in Cyber Security |
| Rochester Institute of Technology- Dubai | Bachelor/Master of Science in Computing Security |
| UAE University | Bachelor/Master of Science in Information Security |
| University of Dubai | Master of Science in Cyber Security |
| University of Fujairah | Bachelor of Information Technology<br>Concentration: Networking and Security |
| University of Science and Technology of Fujairah | Bachelor of Science in Information Technology<br>Concentration: Cyber Security |
| University of Sharjah | Bachelor/Master of Science in Cybersecurity Engineering |
| University of Wollongong in Dubai | Bachelor of Computer Science<br>Concentration: Cyber Security |
| Zayed University | Bachelor of Science in Information Technology<br>Concentration: Security and Network Technologies |
| | Master of Science in Information Technology<br>Concentration: Cyber Security |

Therefore, a wide array of specialized cybersecurity programs across different universities in the UAE reflect the nation's commitment to addressing the growing demands of digital security. These programs, ranging from bachelor's to master's degrees, consistently emphasize critical learning outcomes such as the ability to analyze and solve complex cybersecurity problems, design and implement secure computing-based solutions, and effectively communicate within professional contexts. Moreover, they aim to instil in graduates a strong sense of professional responsibility, ensuring ethical and legal compliance in cybersecurity. Through a blend of theoretical knowledge and hands-on laboratory experiences, these programs prepare students for diverse roles, including security analysts, cyber security specialists, and digital forensic analysts. By focusing on cutting-edge topics such as network security, digital forensics, ethical hacking, and cryptography, these educational offerings are aligned with regional and global cybersecurity challenges, equipping graduates to contribute significantly to the security needs of the UAE.

### *4.2.2 Identified Gaps and Challenges Based on International Standards*

While many universities offer comprehensive programs in cybersecurity, there is an opportunity to ensure that curriculum development and updates are closely aligned with international standards such as ISO/IEC 27001, ISO/IEC 27002, and NIST frameworks [157]-[159]. This alignment helps prepare students with globally recognized best practices and knowledge, enhancing their employability and effectiveness in addressing cybersecurity challenges. Some programs may emphasize theoretical knowledge over practical application. International standards like NIST SP 800-50 and CIS Controls stress the importance of hands-on experience in dealing with real-world cybersecurity scenarios [160], [161]. To bridge this gap, universities could enrich their programs by incorporating more practical labs, simulations, and internship opportunities with industry partners.

The rapidly evolving nature of cyber threats requires that educational programs remain up-to-date with the latest developments in the field. This presents a challenge in keeping the curriculum in line with the dynamic landscape of cybersecurity, as outlined in frameworks like ISO/IEC 27032 [162]. Universities need to implement mechanisms for regular/continuous curriculum reviews and updates to incorporate new threats,

technologies, and countermeasures. While specialized programs focus on training future cybersecurity professionals, there's a broader need for awareness and training across all university programs. This aligns with the emphasis on awareness and training found in ISO/IEC 27002 and NIST frameworks [158], [159], suggesting that cybersecurity awareness should be an integral part of education for all students, regardless of their major, to promote a security culture. Cybersecurity education must also address ethical and legal aspects of information security, as highlighted in standards like NIST SP 800-53 [163]. Programs could be enhanced by integrating courses that cover ethical hacking guidelines, data protection laws, and the implications of cybersecurity measures on privacy and individual rights.

Cybersecurity challenges often intersect with other domains, such as law, business, and policy. An interdisciplinary approach to cybersecurity education, suggested by the comprehensive view of standards like ISO/IEC 27032 [162], can equip graduates with a broader understanding of how cybersecurity integrates with other fields. This approach can prepare students to develop more holistic security solutions. Aligning academic programs with professional certifications (e.g., CISSP, CISM) can add value to a graduate's qualifications. Incorporating certification preparation into the curriculum can address the gap between academic education and professional practice, ensuring that graduates are ready to meet industry standards. Given the global nature of cyber threats and the specific challenges faced in the Gulf region, cybersecurity education programs in the UAE should incorporate both global perspectives and regional considerations into their curriculum. This dual focus would prepare students to operate effectively internationally while addressing local cybersecurity needs and regulations.

# Chapter 5: Cybersecurity Awareness Study in the UAE

This chapter delves into a comprehensive study conducted to assess cybersecurity awareness, practices, and experiences among individuals in the UAE. Utilizing a meticulously designed survey executed in both Arabic and English versions, this study aims to uncover the depth of knowledge, the prevalence of cybersecurity best practices, the experiences of individuals with cybersecurity threats, and their preferences for acquiring cybersecurity knowledge. With a total of 500 responses collected—428 from the Arabic version and 72 from the English version—through Google Forms, the survey was randomly distributed to ensure a broad representation of the population. Survey participation was voluntary and anonymous, emphasizing the importance of honest and uninhibited feedback. Beginning with an analysis of participant demographics to establish the contextual backdrop of the study, the chapter progresses to dissect survey findings across key areas: knowledge and awareness of cybersecurity, prevailing cybersecurity practices and beliefs, experiences with cybersecurity threats, and preferences for learning about cybersecurity. This exploration aims to illuminate the current state of cybersecurity awareness among the UAE populace, identifying strengths and uncovering gaps in knowledge and practices, thereby providing actionable insights for enhancing cybersecurity awareness and education.

## 5.1 Participant Demographics

The survey garnered 500 participants from different emirates in the UAE. Most of the respondents were from Abu Dhabi, contributing 451 participants. Dubai followed with 19 participants, Sharjah with 11, and Fujairah with 7. The emirates of Umm Al Quwain and Ras Al Khaimah had a modest representation, with 2 and 9 participants, respectively, while Ajman had the least, with only 1 participant as represented in Figure 4.

| Emirate | Number of Participants |
|---|---|
| Abu Dhabi | 451 |
| Dubai | 19 |
| Sharjah | 11 |
| Ajman | 1 |

| Emirate | Number of Participants |
|---|---|
| Umm Al Quwain | 2 |
| Ras Al Khaimah | 9 |
| Fujairah | 7 |

Total Number of Participants: 500

Figure 4: Number of Participants per Emirates

Figure 5 displays the demographic breakdown of the survey participants based on their gender and age. Among the respondents, 68.2% (341 individuals) are male, while 31.6% (158 individuals) are female. Only one participant, representing 0.2%, preferred not to disclose their gender. In terms of age distribution, the 35-44 age group had the highest number of participants, with 248 individuals, followed by the 18-24 and 45-55 age groups, with 72 and 76 participants, respectively. The 25-34 age group had 100 participants. However, the survey had limited participation from the older population, with only four individuals from the 55+ age group responding.

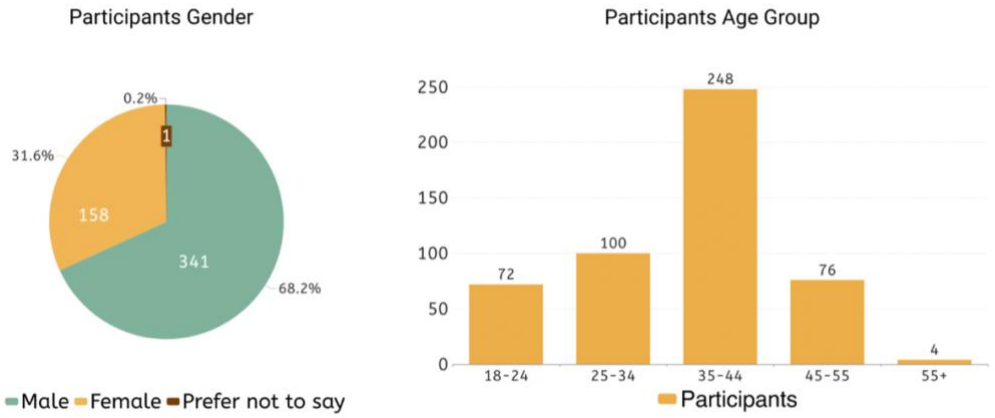



Figure 5: Participants Age and Gender

The participant occupational demographics within the cybersecurity awareness study present an insightful composition of the survey cohort. The majority of respondents, as illustrated in Figure 6, 340 individuals, accounting for 68%, are identified as employees, suggesting significant engagement from the working population. Bachelor students represent the second-largest group, comprising 53 participants, or 10.6% of the total participants. Postgraduate students are also notable contributors to the survey, with 46 respondents making up 9.2%. The survey also includes the perspectives of the unemployed, who constitute 5.2% of the respondents with 26 participants, and retirees, who form 7% of the respondents with 35 individuals. The varying occupational backgrounds of the participants provide a diverse cross-section of the population, offering

a comprehensive overview of cybersecurity awareness across different segments of society in the UAE.

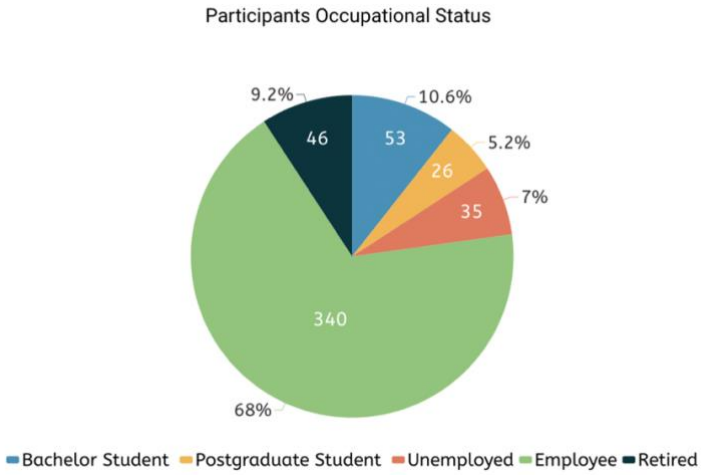



Figure 6: Participants Occupational Status

## 5.2 Survey Findings

### *5.2.1 Knowledge and Awareness of Cybersecurity*

Figure 7 illustrates the participants' self-assessed awareness of information security or cybersecurity. A majority, 58.6%, affirmed their understanding, indicating a positive awareness level within the sample. Conversely, 24.2% of respondents were uncertain about their knowledge, while 17.2% explicitly indicated a lack of understanding. This distribution highlights a significant portion of the sample with a confident grasp of cybersecurity, yet also underscores the need for increased educational efforts for those uncertain or unaware of the concept.

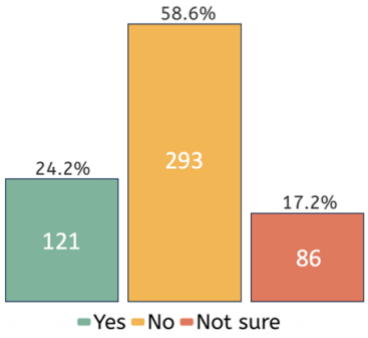



Figure 7: “I know what information security, or cybersecurity, means”

In the survey, participants were asked to select the best definition of cybersecurity. The response results are shown in Figure 8. The option that received the most responses, with 180 individuals choosing it, was (b) "Ensuring the privacy of personal information online." as the best definition of cybersecurity, suggesting that many people equate cybersecurity with protecting personal data. The technically comprehensive option (c), "Securing computer systems against unauthorized access or attacks," which truly encapsulates the breadth of cybersecurity, was the second most popular choice with 136 responses. Option (a), "Protection of physical assets from theft or damage," although more related to physical rather than cyber aspects, received 132 responses, indicating some confusion about the scope of cybersecurity. The least favored definition, with 52 responses, was (d) "Preventing viruses from infecting computer networks," a critical function of cybersecurity but not representative of its entirety.

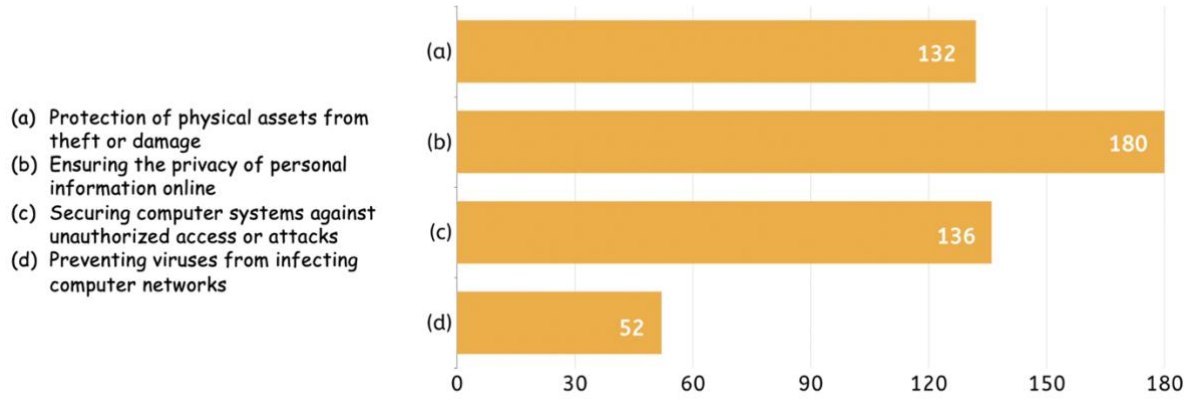



Figure 8: "Which of the following is the best definition of cybersecurity?"

Figure 9 illustrates survey responses to where individuals first heard about cybersecurity. The bar chart indicates that social media is the leading source of initial cybersecurity awareness, with 220 respondents crediting these platforms, underscoring their influential role in information dissemination. Personal networks, through family and friends, are the second most cited source, with 119 acknowledgements emphasizing the importance of interpersonal communication in spreading knowledge. Work environments rank third, with 88 individuals pinpointing their professional settings as the point of introduction, reflecting the priority given to cybersecurity in the workforce. Education at

universities has informed 31 participants, while online courses have played a part for 12 respondents, indicating avenues of structured learning. Surprisingly, only 6 have mentioned school as their source. Alarmingly, 24 respondents have never heard of cybersecurity, highlighting a significant awareness gap that must be addressed.

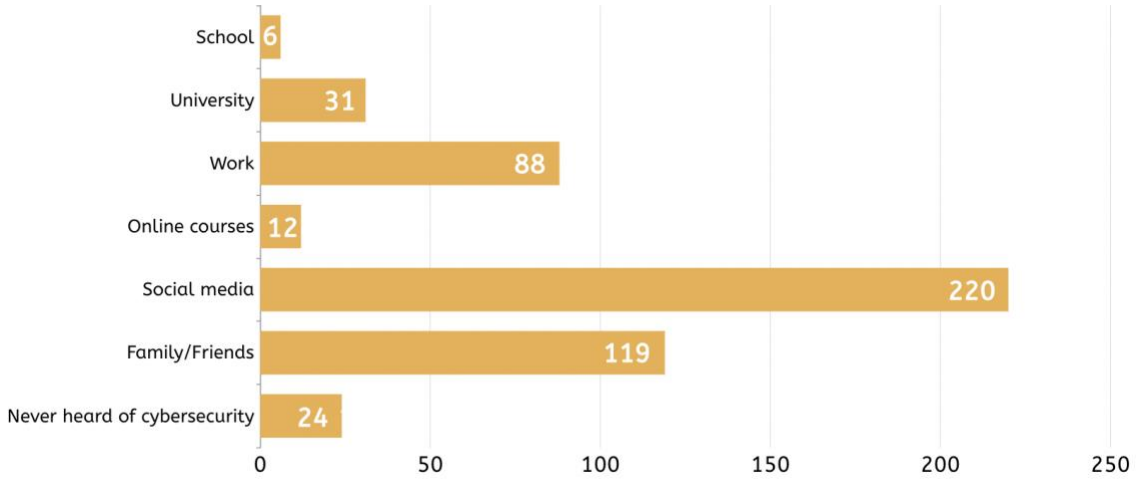



Figure 9: "Where did you first hear about cybersecurity?"

Figure 10 presents the results of a survey question regarding what participants believe should be included in a strong password. The bar chart indicates that the majority, with 227 selections, are aware that a strong password should be short enough to remember easily. This suggests a common misconception, as shorter passwords may often be weaker.

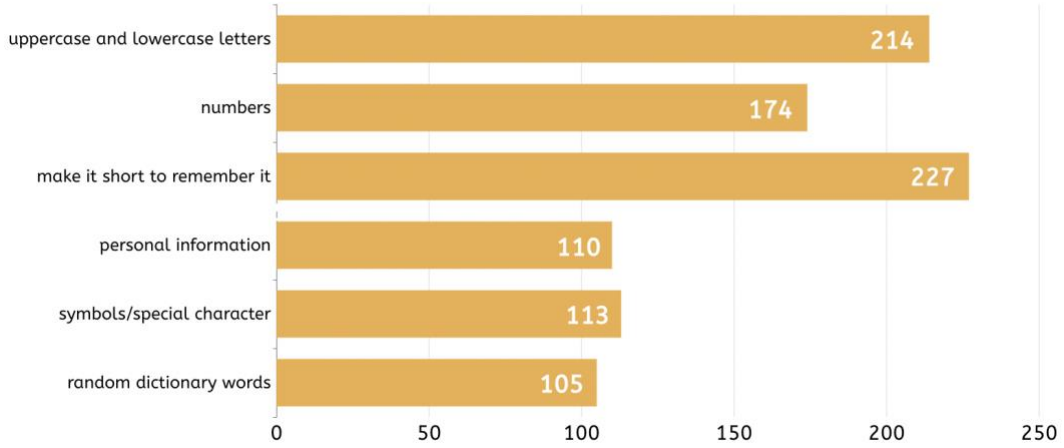



Figure 10: “I am aware that strong passwords must include”

The use of both uppercase and lowercase letters is recognized by 214 participants as a characteristic of strong passwords, showing a good understanding of the importance of letter case variation for password strength. Numbers are also acknowledged by 174 respondents, highlighting their awareness of numerical inclusion for complexity. Symbols and special characters are noted by 113 participants, and personal information is surprisingly considered by 110 respondents despite it typically being advised against for security reasons. Lastly, 105 individuals recognize the use of random dictionary words as a component of strong passwords, which, while contributing to memorable passwords, may expose users to dictionary attacks if not combined with other complex elements.

The pie chart in Figure 11 depicts responses to the question of how often passwords should be changed. The largest group, consisting of 227 individuals, believes passwords should be changed yearly, representing the most common interval chosen. The next significant group, with 119 individuals, thinks a 6-month interval is appropriate for changing passwords. A smaller number, 66 respondents, advocate for a 3-month password change cycle. Both the 5-month and 2-3-year intervals are the least favored, with each having 26 individuals supporting them. Lastly, 39 individuals feel that there is no need to change passwords if they are strong, representing the smallest segment of responses.

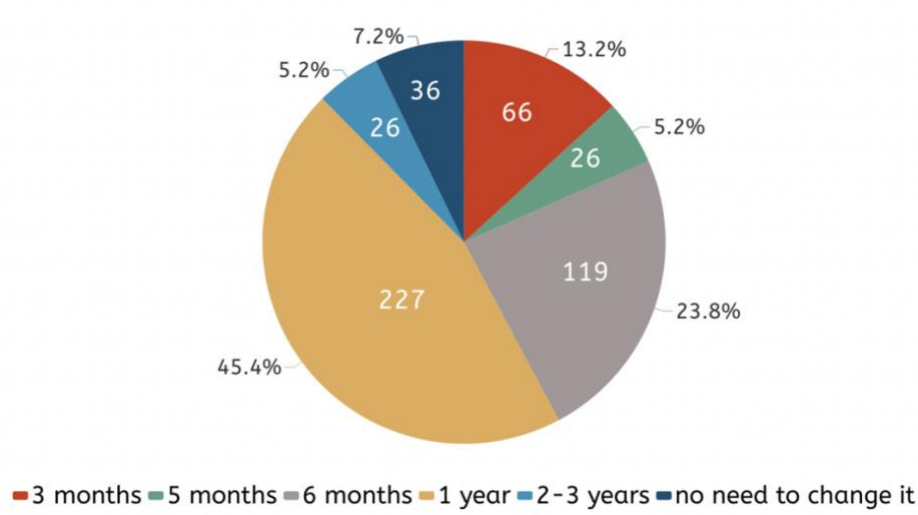



Figure 11: "I am aware that passwords need to be changed every"

In Figure 12, participants responded to the question regarding the definition of phishing. Option (c), which correctly defines phishing as a fraudulent attempt to obtain

sensitive information by pretending to be a trustworthy entity, garnered 133 responses. This indicates a recognition of phishing among some participants. However, the majority, with 207 responses, incorrectly chose option (a), suggesting a misconception that phishing involves hackers gaining physical access to a computer system. Option (b), describing a method of protecting data through encryption, also received 100 incorrect selections, while option (d), referring to anti-virus software, was chosen by 60 respondents, further highlighting misunderstandings about phishing versus other concepts.

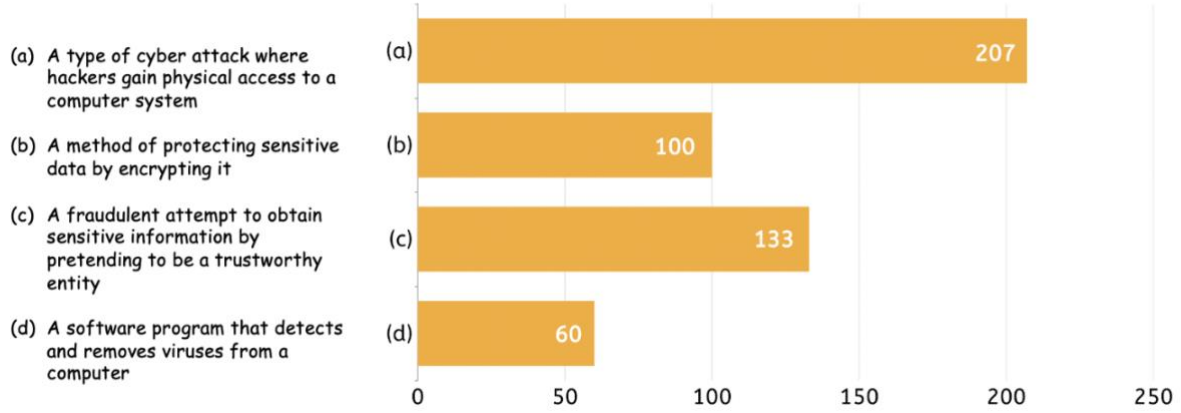



Figure 12: “What is phishing?”

In Figure 13, the survey explored participants' understanding of phishing attacks. The most common response, chosen by 265 individuals, incorrectly identified sending spam emails to a large group of people as a phishing attack. While spam can be a method used in phishing, it is not exclusively so. A significant number of participants, 119, also incorrectly identified gaining unauthorized access to a computer network as an example of phishing. Only 69 respondents correctly identified pretending to be a legitimate organization to obtain sensitive information as phishing, which is the essence of such attacks. Lastly, 47 participants mistakenly believed that manipulating search engine results to display fake websites falls under the definition of phishing, which suggests a broader misunderstanding of the term among the survey participants.

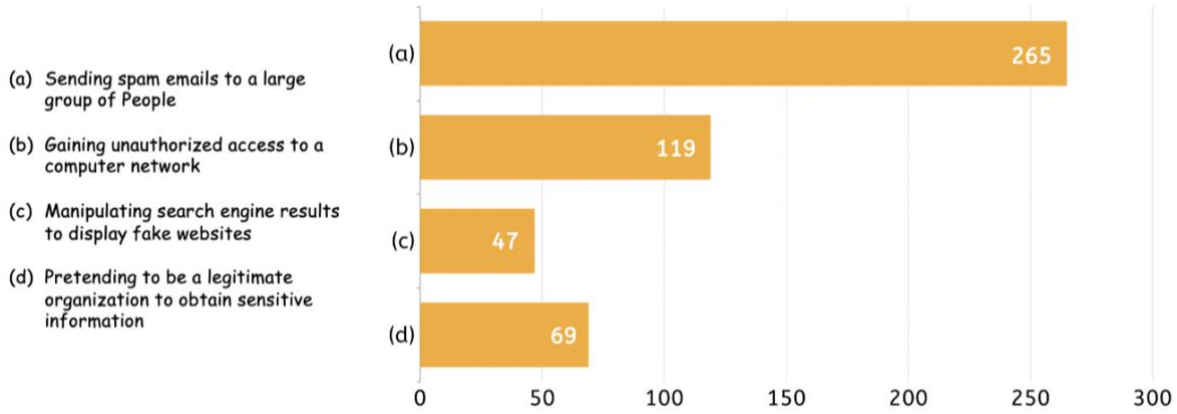



Figure 13: "Which of the following is an example of a phishing attack?"

Figure 14 presents the responses to the query, "What is malware?" The highest number of participants, 206 individuals, incorrectly chose option (a), suggesting a misunderstanding of malware as a hardware component that enhances computer performance. Another 139 participants incorrectly identified malware as software used to protect against cybersecurity threats, which is the opposite of what malware represents. A relatively closer number, 121 respondents, correctly identified the malware as unwanted software designed to harm or infiltrate a computer system. Only 34 individuals mistakenly selected option (d), a security protocol used to encrypt network communications, which is not related to malware. These responses indicate a significant variance in the understanding of what malware is among the survey participants.

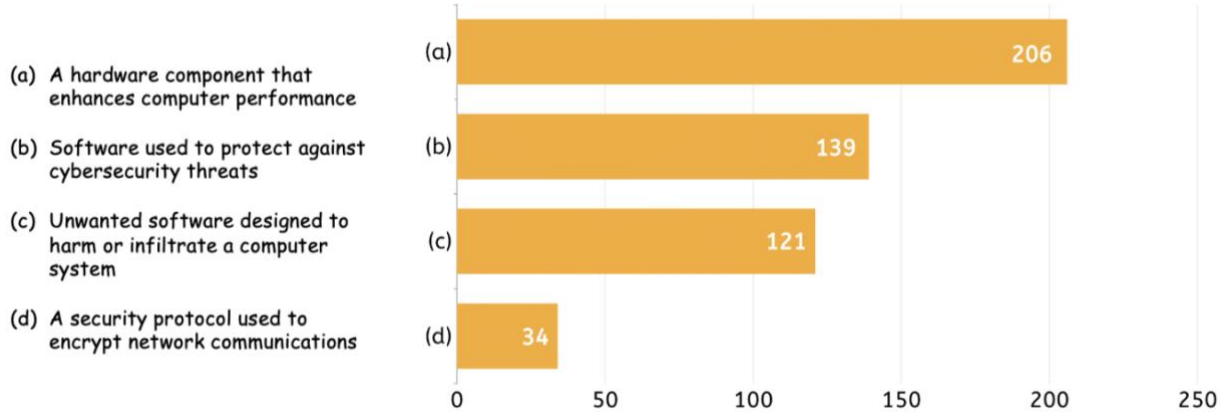



Figure 14: "What is malware?"

Figure 15 indicates the participants' understanding of what constitutes a firewall based on the survey question. A significant number of participants, 183 individuals, mistakenly believed that a firewall is a physical barrier used to protect computer systems from physical damage. Another large group of 178 participants incorrectly identified a firewall as software that scans and removes viruses from a computer. The correct definition, a security measure that restricts unauthorized network traffic, was recognized by 86 individuals. Lastly, 53 respondents inaccurately chose the option of a firewall as a tool to prevent unauthorized access to email accounts. This distribution of responses highlights a common confusion about the function of a firewall, with a notable portion of the participants not identifying its true purpose as a network security system that filters incoming and outgoing traffic.

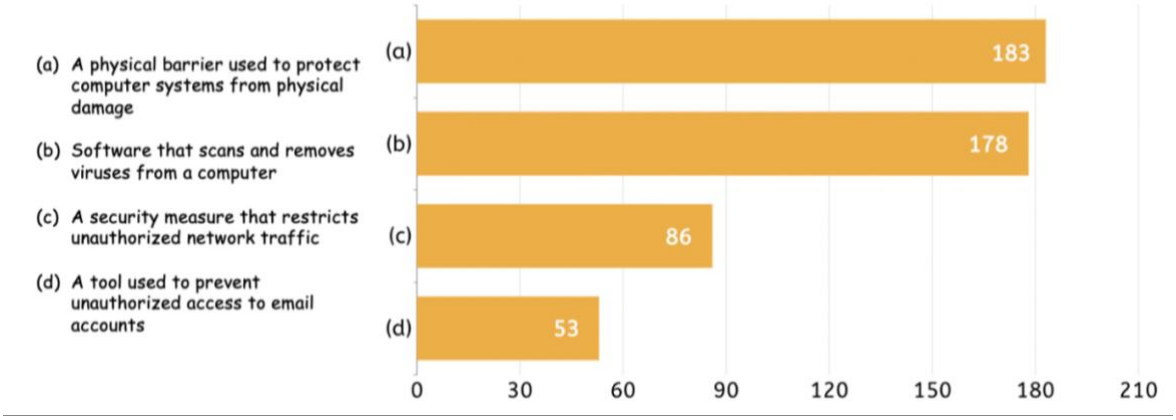



Figure 15: "What is a firewall?"

*5.2.2 Cybersecurity Practices and Beliefs*

Figure 16 reflects participants' cybersecurity practices and beliefs concerning the trustworthiness of files received from unknown sources. An overwhelming majority of 390 individuals 'strongly agree' that they do not trust any files received from people they do not know, highlighting a high level of caution exercised by these respondents. A further 77 participants 'agree' with this cautious stance, adding to the significant proportion of individuals who prioritize security when dealing with unsolicited digital content. Neutral responses are minimal, with only 15 individuals not committing to either trust or distrust, suggesting that most have a definitive opinion. A small minority of 7 'disagree' and an even smaller number of 11'strongly disagree', indicating they might be more open to

accessing files from unknown senders, which could potentially expose them to cybersecurity risks.

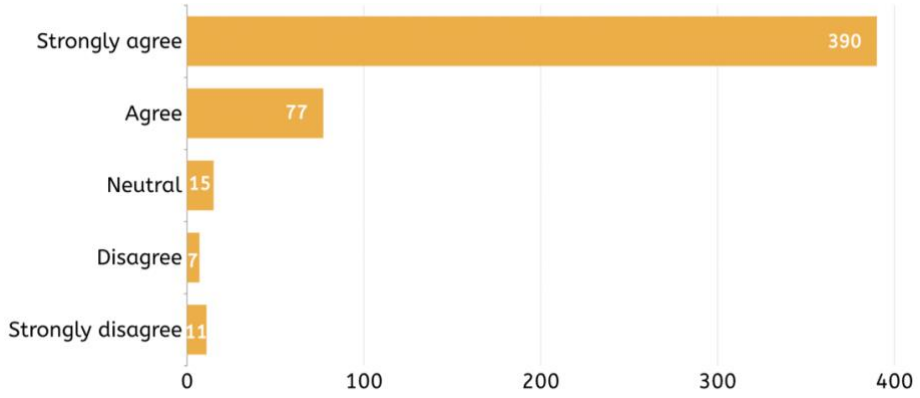



Figure 16: "I don't trust any file I receive from people I don't know"

Figure 17 displays participant attitudes towards opening unexpected files from known contacts, revealing a varied approach to such cybersecurity scenarios. While 276 respondents indicated they would 'agree' to open such files, reflecting a certain level of trust in their sources, 62 individuals 'strongly agree', showing an even greater level of confidence. However, a noteworthy segment of participants exercise caution: 47 'strongly disagree' and 39 'disagree' with opening files from familiar sources without verification, recognizing the risk of contact compromise where attackers may exploit trusted relationships. The 76 'neutral' respondents suggest a group that is either undecided or weighing the risks of such actions.

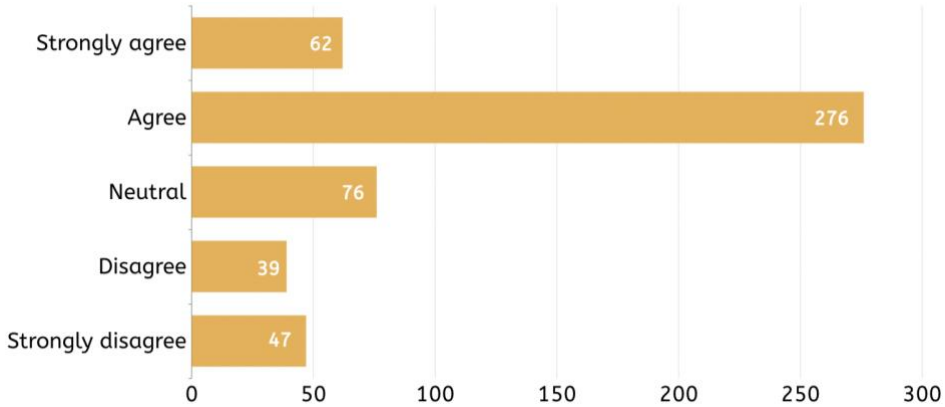



Figure 17: "I trust and open any unexpected file I receive from people I know"

Figure 18 presents the responses to the security of entering private information (e.g., date of birth, Identification Number) on sites that begin with "http://". A notable majority, 302 individuals, agree that it is safe, while 61 strongly agree, indicating a significant portion of participants may not recognize the potential risks associated with non-secure protocols. On the other end, 43 respondents are in strong disagreement, and 30 disagree, suggesting an awareness of the security vulnerabilities of HTTP sites. With 64 participants remaining neutral, there appears to be a lack of consensus or understanding about the security implications of HTTP and HTTPS protocols, highlighting a critical area for cybersecurity education and awareness.

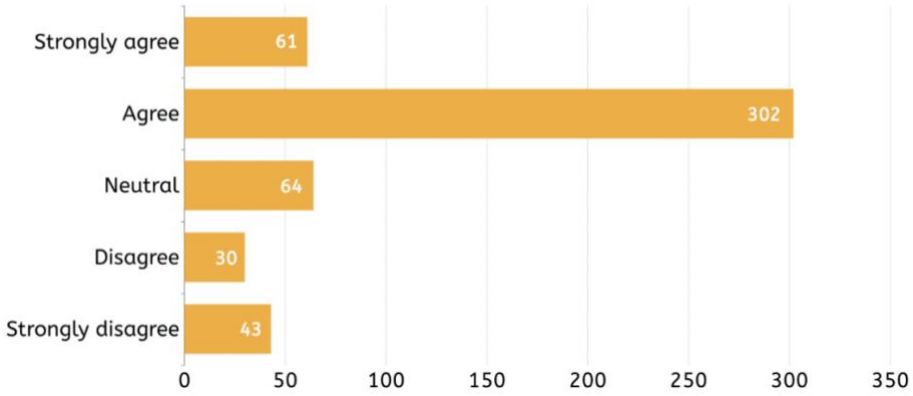



Figure 18: "It is safe to enter your private info on a site that starts with "http:// ""

Figure 19 presents survey responses to a hypothetical scenario involving an unsolicited pop-up advertisement (Scenario: "You're browsing on a random site, and a pop-up appears offering free access to Netflix. What is the most secure action to take?"). The majority (365 individuals) selected the most secure option by closing the pop-up and not proceeding. Conversely, 50 respondents indicated a willingness to follow the pop-up's instructions, potentially exposing themselves to cyber threats. Additionally, 63 individuals would ignore the pop-up entirely, potentially leaving them vulnerable if it's a malicious site. Interestingly, 22 individuals, attempting to be helpful, would share the pop-up link with friends. However, this action could inadvertently expose their contacts to risk if they unintentionally click the link and/or provide their personal information. The range of responses to this question underscores diverse approaches to cybersecurity practices and the need for heightened awareness of secure online behavior.

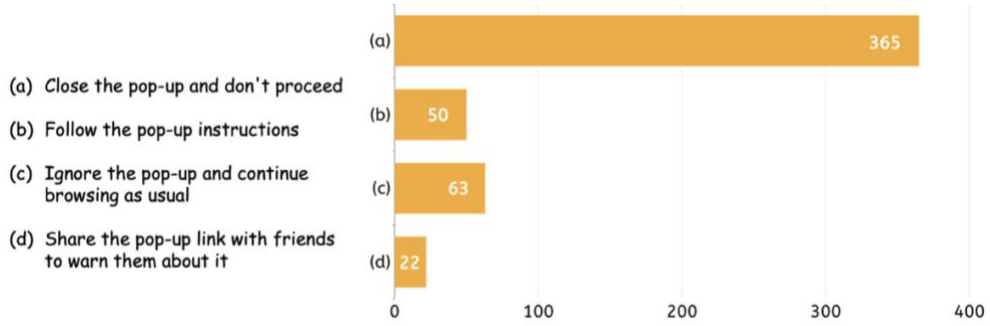



Figure 19: "What is the most secure action to take?"

Figure 20 explores participants' responses to receiving an email supposedly from Amazon support requesting an immediate password reset. While the majority (413) wisely chose to ignore the email, potentially avoiding a phishing scam, a concerning number (87) indicated they would follow the instructions and change their password, highlighting the need for continued education on identifying and handling suspicious emails. Overall, the majority of participants are aware of the dangers of phishing emails. However, there are still a significant number of people who may be susceptible to these scams.

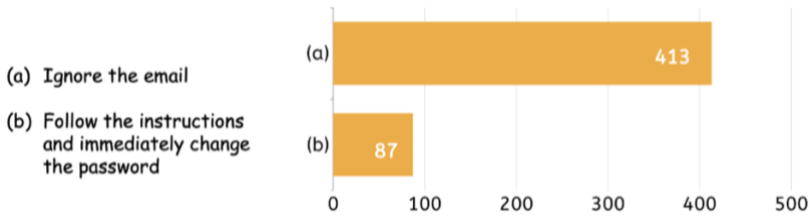



Figure 20: Participants' Responses to a Potential Phishing Attempt Scenario

Figure 21 explores participant responses regarding a found USB device in a university/work hallway. The majority (310 participants) demonstrated security awareness and delivered it to the IT department, as USB devices could contain malware that could infect computers and steal data. However, 50 participants would attempt identification by plugging it into a computer, which is the least secure option, as it could expose the user's computer to malware if the USB drive is malicious. 140 participants would leave it in the hallway so whoever loses it can find it; while this may seem helpful, it is also not recommended, as the USB drive could be picked up by someone who intends to misuse it.

The figure shows that most participants know the risks associated with USB devices. However, a significant number of people are still not taking the most secure actions, highlighting the need for continued education on safe handling practices for USB devices.

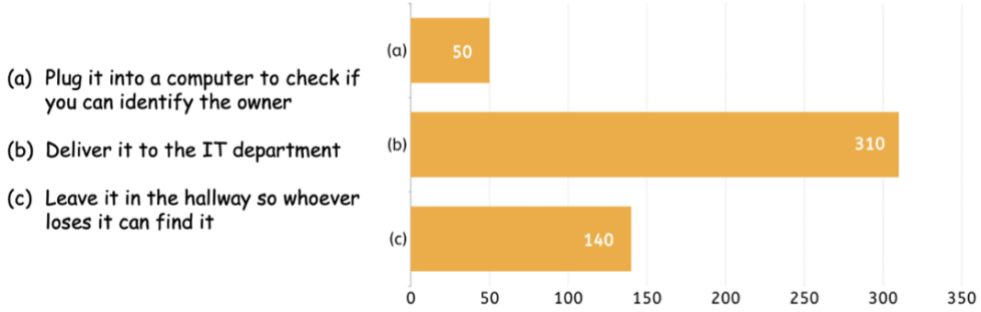



Figure 21: Participants' Behavior in Handling the Found USB Device

Figure 22 explores participant responses to identifying trustworthy online shopping websites. The majority (178 participants) demonstrated awareness of cybersecurity practices by prioritizing independent research to verify the website's reputation. 138 participants will look for a website address that starts with "https://.". This is a good indicator that the website uses encryption to protect your data, but it is not enough to guarantee the website's legitimacy on its own. On the other hand, a number of participants relied solely on less reliable factors: website seals (94 participants) and customer reviews (90 participants). While these factors can indicate security, they are easily manipulated and insufficient on their own, which highlights the need for comprehensive education on evaluating online store legitimacy.

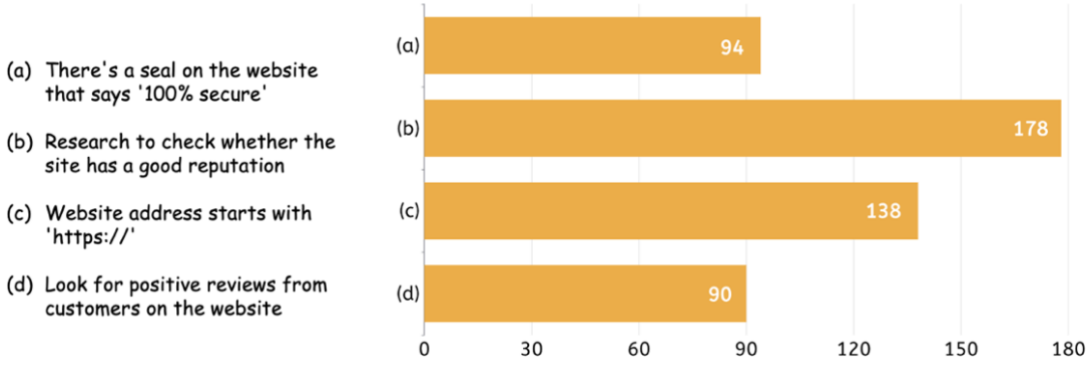



Figure 22: Identifying Trustworthy Online Shopping Websites

*5.2.3 Experiences with Cybersecurity Threats*

Figure 23 reveals the cybersecurity incidents encountered by participants and their family members. A significant number of respondents, 228 individuals, experienced not receiving items ordered online, indicating a prevalent issue with online shopping fraud. The second most common experience, with 120 responses, was receiving suspicious calls or messages asking for personal information, a classic sign of phishing attempts. Close behind, with 116 individuals, were those who received emails or messages prompting them to verify an account or pay for a service, another common phishing tactic. Account hacking is also a notable concern, with 96 participants reporting their social media accounts being compromised. Online harassment or cyberbullying has affected 53 respondents, while 98 individuals have encountered someone attempting theft or fraud under the guise of seeking help, and 79 have been victims of fraudulent online transactions.

| Situations that participants or their family members have ever been victims of | Number of Participants |
|---|---|
| Helped someone who randomly asked for help, and it turned out they were attempting theft or fraud | **98** |
| Your social media account has been hacked | **96** |
| Ordered something online and never received it | **228** |
| Your device has been locked by someone and asked you to pay a specific amount of money | **46** |
| Received an email or SMS message asking you to verify your account or to pay for a service | **116** |
| Experienced identity theft or unauthorized use of your financial accounts | **21** |
| Encountered unauthorized access or a breach of your personal data | **27** |
| Became a victim of online harassment or cyberbullying | **53** |
| Received a suspicious phone call or message requesting personal information | **120** |
| Shared sensitive personal information online unintentionally | **33** |
| Became a victim of fraudulent transactions online | **79** |
| Had your personal information exposed in a data breach | **19** |

Figure 23: Cybersecurity Incidents Encountered by Participants/Their Family Members

There are lower frequency incidents, such as 46 individuals whose devices were locked by ransomware, demanding payment, and 33 who have unintentionally shared

sensitive information online, showing lapses in information security practices. Identity theft and financial account misuse were reported by 21 participants, while 27 faced unauthorized access or breaches of personal data, and 19 had their personal information exposed in data breaches. These insights underscore the diverse and prevalent cybersecurity challenges individuals and their families face, highlighting the importance of awareness of digital security measures.

### *5.2.4 Learning Preferences*

The participants' preferences for learning about cybersecurity, as represented in Figure 24, showcase a trend towards interactive and formal education settings. Public educational workshops are the most favoured method, with 361 individuals selecting this option, indicating a strong interest in community-based learning initiatives. Close behind are work workshops and university programs, with 334 and 333 selections, respectively, suggesting that professional and academic environments are considered valuable for acquiring cybersecurity knowledge. Despite the widespread use of digital platforms, online courses, educational applications, and social media platforms are less preferred, with 89, 86, and 104 selections, respectively. This might reflect a desire for more personalized, hands-on learning experiences or indicate that the quality and trustworthiness of information from these sources are perceived as variable.

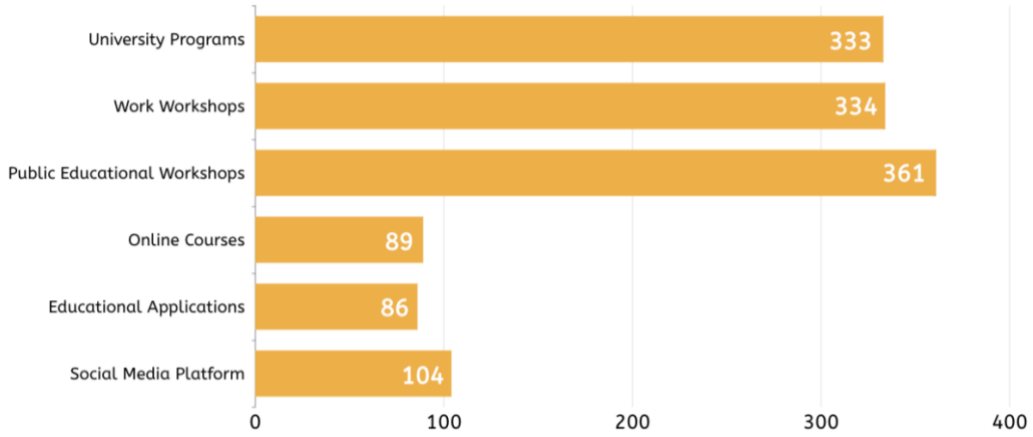



Figure 24: Learning Preferences

At the end of the survey, participants were asked about the desirable features of a cybersecurity educational app. Participants provided various suggestions, reflecting the

need for foundational and advanced security knowledge. Key features included mandatory fundamentals training for beginners and non-IT professionals and awareness of common frauds to aid in identifying credible organizations. Participants expressed the need for guidance on immediate steps following data compromise, techniques for personal data theft prevention, updates on recent cyberattacks, and methods to check for device intrusion, particularly regarding camera hacking. The ability to report cybercrimes and access emergency assistance if hacked was also highlighted. Users desired a 'shield' for device protection, practical training, and breakdowns of cybersecurity certifications. Interactive components like tests to evaluate responses to phishing attempts and the inclusion of new scamming methods were also mentioned. Educational content that is accessible, engaging, and caters to all ages was significant, with suggestions for a simple user interface, clear and concise explanations, and both auditory and visual learning options. Participants also wanted a search engine to verify the safety of websites and a comprehensive and easy-to-use app that offers lists of available workshops or courses in the UAE. Practical exercises to complement theoretical materials were also requested, indicating a preference for hands-on learning experiences.

### 5.3 Discussion

The participant demographics section of the cybersecurity awareness survey provides a foundational understanding of the study's sample representation. Drawing from a varied participant pool, the survey includes a range of educational backgrounds, from bachelor and postgraduate students to employees and retirees, reflecting a rich tapestry of life stages and professional statuses. Geographically, the survey captures responses from across the emirates, with a significant concentration from Abu Dhabi, thus ensuring a breadth of perspectives within the UAE. Gender distribution among participants shows a balanced representation, while the age groups indicate a skew towards the younger and middle-aged cohorts, which are typically more engaged with digital technologies. This demographic overview sets the stage for analyzing the subsequent sections, offering insights into the cybersecurity awareness levels that may be influenced by factors such as age, occupation, and regional distribution.

The findings from the survey on cybersecurity knowledge and awareness reflect a diverse understanding of cybersecurity among participants in the UAE. While most are aware of cybersecurity and can identify basic principles, there are evident gaps and misconceptions. The survey indicates that social media is a significant source of initial cybersecurity awareness, yet many participants' first understanding of cybersecurity comes from personal networks or professional environments, pointing to a need for more structured educational initiatives. Misunderstandings around the definition of phishing, the true purpose of malware, and the function of a firewall suggest that while there is a baseline awareness, deeper and more accurate knowledge is required. The assumption that strong passwords need only be memorable and the belief that certain ineffective practices are safe, such as infrequent password changes or trusting files from known contacts without verification, demonstrate a critical need for improved cybersecurity education and best practices dissemination.

The survey section on cybersecurity practices and beliefs provides valuable insights into the participants' behavior and perceptions. A large majority exhibit caution with unknown files, affirming good cybersecurity practices. However, an apparent trust is placed in files from known contacts, potentially overlooking the fact that such contacts could be compromised. This points to a nuanced understanding of trust in digital communications. When it comes to website security, many participants seem unaware of the risks associated with non-HTTPS sites, indicating a gap in understanding secure online protocols. Reactions to phishing attempts vary, with most recognizing and appropriately dismissing suspicious emails, but a notable portion would respond, showing a need for better recognition of phishing tactics. Finally, while many would responsibly handle a found USB device by reporting it to IT, others would take less secure actions, underscoring the need for heightened awareness about device security.

The survey findings on experiences with cybersecurity threats paint a detailed picture of the digital risks individuals face in the UAE. It's concerning to note that the most reported issue involves online shopping fraud, reflecting the risks associated with e-commerce. Phishing attacks, whether through suspicious communications or deceptive emails, also emerge as common threats, affecting a significant portion of respondents. The prevalence of social media account hacking underscores the need for stronger account

security practices. Furthermore, the experiences of online cyberbullying and attempted theft or fraud suggest a broader scope of cybersecurity challenges affecting personal well-being. The less frequent, yet serious incidents of ransomware attacks, unintentional information sharing, identity theft, and data breaches signal the complex nature of cybersecurity threats that can have long-term repercussions. These findings highlight the need for robust cybersecurity measures and comprehensive education to enhance the digital resilience of individuals and their families against cyber threats.

# Chapter 6: Comprehensive Synthesis

This chapter serves as a comprehensive synthesis of the significant insights gleaned from the preceding analyses of cybersecurity education gaps and awareness within the UAE. It draws upon the detailed findings from Chapter 4, which scrutinized the current state of cybersecurity education in public schools and universities against international standards, revealing critical gaps and implications for students and cybersecurity specialists. Furthermore, it consolidates the key observations from Chapter 5, which empirically evaluated cybersecurity awareness among various demographics through a structured survey. This chapter aims to merge these findings into a coherent narrative, identifying the specific cybersecurity awareness needs of different segments within the UAE community. It seeks to offer a nuanced understanding of the diverse awareness levels, practices, beliefs, and experiences with cybersecurity threats as reported by participants, thus guiding the development of targeted educational strategies and initiatives that cater to the identified unique needs.

## 6.1 Key Findings and Major Concerns

The examination of cybersecurity awareness in the UAE, as documented in Chapters 4 and 5, has yielded significant insights. Chapter 4's evaluation of the educational landscape revealed that despite the existence of cybersecurity programs, there remains a notable disconnect between the curriculum offered and the practical demands of cybersecurity proficiency, particularly in public schools and universities. This gap in education may hinder the development of fully prepared individuals and cybersecurity professionals capable of tackling the complexities of today's cyber threats. Chapter 5's in-depth survey provided a granular view of the public's cybersecurity awareness. The findings suggest a baseline awareness among participants, but also reveal critical misconceptions and gaps in knowledge. A considerable number of respondents are unsure or misinformed about what constitutes cybersecurity, appropriate practices, and the frequency of encountering cyber threats. Therefore, while there is an existing foundation of cybersecurity awareness in the UAE, the need for enhanced, targeted education is evident. The current awareness levels, coupled with the reported experiences of cyber threats, underscore the urgency for educational reforms that can elevate understanding and

empower individuals with the skills to navigate and secure their digital environments effectively. These reforms should address the identified educational gaps and equip the populace with theoretical knowledge and practical skills to proactively recognize and respond to cybersecurity challenges.

In summary, exploring cybersecurity education and awareness in the UAE reveals critical gaps and challenges, as presented in Chapters 4 and 5. A marked deficiency in foundational cybersecurity knowledge within curricula leads to a general need for more awareness about safe digital practices. Practical skill development is also limited, with scant real-world simulation exercises for students. Cyber ethics and legal frameworks need to be sufficiently covered, leaving students with little understanding of the UAE's cyber laws. Advanced threats and their corresponding defence mechanisms must be adequately addressed, with educational programs often lagging behind the latest developments in AI-driven attacks and other emerging threats. This leads to a shortfall in preparedness for incident response and management, data protection, and privacy adherence, particularly regarding UAE regulations. Furthermore, some university programs need to sufficiently explore the security implications of emerging technologies like blockchain and the IoT. There is also a limitation to aligning educational outcomes with professional cybersecurity certifications and industry standards. Finally, developing critical soft skills pertinent to cybersecurity roles is often overlooked, underscoring the UAE's need for a holistic cybersecurity education and awareness approach.

### 6.2 User Categorization and Cybersecurity Awareness Needs

In Chapter 4, our primary focus encompassed two specific segments: school students under the age of 18, and university students aged 18 and above, specifically those enrolled in cybersecurity-related programs. In contrast, Chapter 5 expanded the scope to include a broader demographic, targeting all individuals above the age of 18, which also includes employees. Given these distinctions, it becomes pertinent to categorize users into distinct groups based on their unique cybersecurity awareness needs. These groups include school students, university students, the general audience, and employees, each requiring tailored cybersecurity education and awareness strategies. Individuals should stay updated

with the latest cybersecurity, enabling a culture of security awareness that evolves with technological advancements and emerging threats.

### *6.2.1 Individuals Aged Under 18*

This section delves into the cybersecurity awareness needs of individuals under 18, a demographic highly engaged with digital technologies yet vulnerable to cyber threats. The focus is on categorizing their needs into two main groups: school students under the age of 14 and those between the ages of 14 and 18, each requiring tailored awareness and education strategies to navigate the digital world safely.

#### *6.2.1.1 School Students Under the Age of 14*

Cybersecurity awareness should prioritize foundational knowledge and practices for school students under 14. This includes, for example, basic concepts such as the significance of strong passwords, understanding personal information privacy, and recognizing common online scams. Awareness among this group of the dangers of oversharing on social media and the basics of safe internet use is crucial. Interactive and engaging methods can effectively convey these concepts, enabling a cautious approach to digital interactions from a young age.

#### *6.2.1.2 School Students Between the Ages of 14 and 18*

For teens aged 14 to 18, cybersecurity awareness should encompass a broader and more detailed context. This includes, for instance, the CIA triad (confidentiality, integrity, and availability) to instill an understanding of fundamental cybersecurity principles, best practices for digital hygiene, awareness of cyberbullying, and strategies for verifying the trustworthiness of online games, applications, and shopping websites. Additionally, discussions on the ethical use of technology and the repercussions of cyber misconduct are essential. Without this knowledge, teens risk exposure to cyber threats and identity theft and could unknowingly contribute to the spread of misinformation or engage in harmful online behaviors.

### *6.2.2 Individuals Aged Above 18*

This section considers the distinct cybersecurity awareness needs of individuals over 18, addressing those without cybersecurity backgrounds and those with specialized knowledge, including university students, graduates, the unemployed, and employees. This demographic often possesses a fundamental understanding of digital technologies; however, some individuals need advanced knowledge and skills to protect against evolving cyber threats.

#### *6.2.2.1 University Students, Graduates, Unemployed*

For university students, graduates, and unemployed individuals without a cybersecurity background, the focus should be on building a robust understanding of fundamental cybersecurity concepts, such as recognizing phishing scams, understanding the importance of data encryption, and practicing safe internet habits. For those in this group interested in a cybersecurity career, providing a clear roadmap for obtaining certifications and highlighting areas of specialization can guide their educational journey and enhance their employability. Conversely, individuals already studying cybersecurity or related fields need to reinforce their knowledge through continuous learning. They should be encouraged to stay updated on the latest cybersecurity trends, such as AI-driven scams, and understand the evolving threat landscape. Additionally, guidance on pursuing professional certifications can assist them in specializing further and preparing for advanced roles in the cybersecurity workforce.

#### *6.2.2.2 Employees*

Employees, regardless of their cybersecurity background, must be equipped with the knowledge to protect personal and organizational digital assets. The basic cybersecurity context for those without a cybersecurity background should include identifying potential cyber threats, secure password practices, and the safe handling of confidential information, etc. A more specialized context should be available for employees with a cybersecurity focus, including advanced threat detection, incident response strategies, implementing cybersecurity policies within their organizations, etc. Continued education is necessary for all employees to adapt to new cybersecurity

challenges, including AI-driven threats, representing a significant and rapidly evolving risk. Regular updates, cybersecurity news feeds, and professional development opportunities can help individuals stay informed and ready to respond to new types of cyberattacks effectively.

In conclusion, through careful investigation, we have categorized the UAE community into distinct groups, each with unique cybersecurity awareness needs. From school students under 14 to high school students aged between 14 and 18, university students, graduates, the unemployed, and employees, each demographic requires tailored cybersecurity education and awareness strategies. This chapter has underscored the critical need for foundational cybersecurity knowledge, practical security skills, understanding of cyber ethics and legal aspects, awareness of advanced threats, and the importance of incident response and management among these groups. Additionally, it highlighted the necessity for ongoing education on data protection, privacy, secure coding practices, and the security implications of emerging technologies.

# Chapter 7: Development of An AI Mobile Application

This chapter delves into the development of an AI-enhanced mobile application tailored to improve cybersecurity awareness across diverse demographics within the UAE. It begins by analyzing the essential cybersecurity awareness needs, detailing the development and design processes to create a user-centric educational tool. The application targets four primary user categories: children under 14, teenagers between 14 and 18, adults over 18, and employees, offering content tailored to each group's unique learning needs and cybersecurity awareness levels. By integrating interactive quizzes, educational content, and AI-powered assistance, the application aims to elevate users' cybersecurity understanding, from basic concepts to advanced practices.

## 7.1 Analysis

The application focuses on equipping individuals with the needed cybersecurity awareness through a mobile application. The application will focus on evaluating and providing comprehensive cybersecurity education content to raise the level of cybersecurity awareness among individuals. As presented in Figure 25, the mobile application is designed for four main categories: users under 14 (elementary and middle school students), users between 14 and 18 (high school students), users above 18 (university students and graduates/unemployed), as well as employees. Each user in each category will be assigned to beginner, intermediate, or advanced levels based on their cybersecurity knowledge test results; however, the users will have the option to access higher levels within the same category.

- Beginners level: This level will cover the basic non-technical introductory information to help users understand the fundamental concepts of cybersecurity awareness.
- Intermediate level: Users in this level will have access to a well-rounded learning experience with both non-technical and technical content.
- Advanced level: This level is tailored for users with prior cybersecurity knowledge; the material for this level is more specialized, offering a solid grounding in cybersecurity awareness.

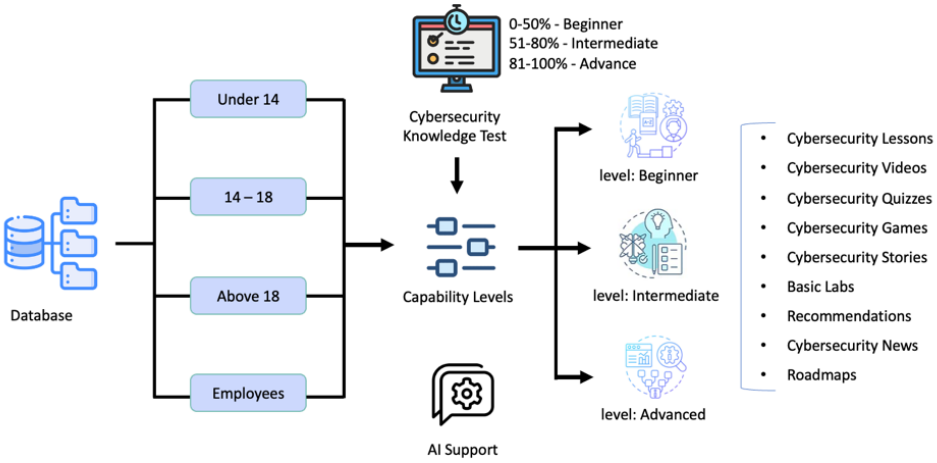



Figure 25: Application Overview Structure

The application content will include lessons, videos, quizzes, scenarios, stories, exercises, daily news, roadmaps, security and privacy tips and recommendations that focus on the following domains: information security, application security, network security, could security, data security, computer/digital forensics, incident responses, end-user behaviors, etc. The tiered approach has been designed to cater to the unique learning pace of every user. It enables them to initiate the learning process from the foundation and gradually advance their knowledge or make quick progress if they already possess prior knowledge. The structured path ensures a continuous learning experience and helps develop essential cybersecurity awareness. The application includes quizzes and evaluation tests specified for each category to measure users' progress effectively. Further, the application features an AI powered by OpenAI to offer accurate and helpful responses to users related to cybersecurity and application content.

## 7.2 Design and Development

### *7.2.1 Users Login / Sign up Page*

The application interface is designed to offer a user-friendly experience. It begins with a login page with fields for email and password, links for creating a new account, and password retrieval. The account registration module is straightforward, gathering information such as username, email, password (with confirmation), date of birth, and occupation to ensure a detailed user profile. Based on the registration information, the users will be categorized into four categories: users under 14, users aged between 14 and

18, users above 18, and employees. Figure 26 presents the login and signup pages, illustrating the application's user-friendly entry points.

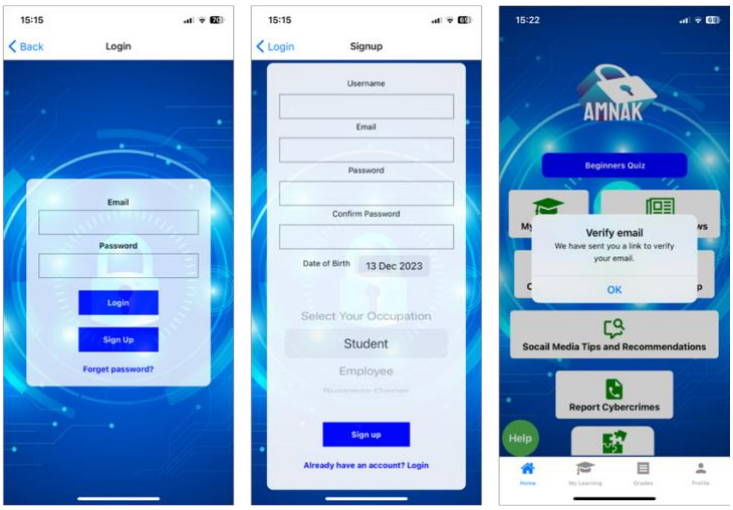



Figure 26: Login/Sign Up Page

Once the user logs in, a beginning evaluation quiz, as presented in Figure 27, will be shown to gauge the user's cybersecurity knowledge; this interactive test features multiple-choice random questions designed to assess users' understanding of cybersecurity. Based on the users' results, they will be assigned to beginners, intermediates, and advanced levels. The quiz interface is intuitive, with straightforward navigation buttons to move between questions and submit answers.

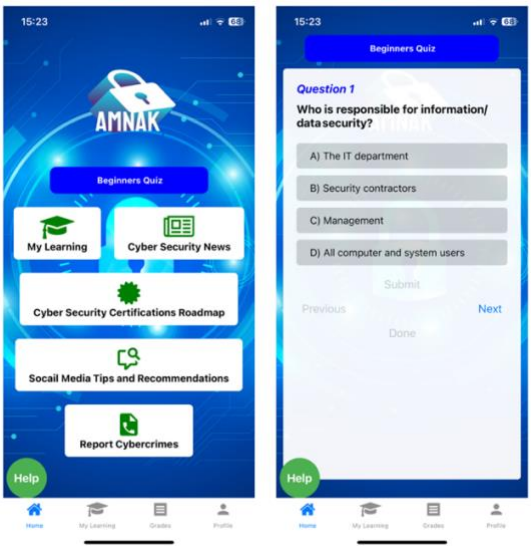



Figure 27: Beginning Test

### *7.2.2 Application User Categories (My Learning Page)*

The application's homepage offers universal access to its various features, while the "My Learning" section is customized to fit different user groups, providing age and role-specific educational content. Younger school students can explore interactive materials such as videos, stories, and exercises organized into beginner, intermediate, and advanced levels. University students, graduates, or unemployed individuals above 18 are offered structured cybersecurity lessons across the same skill levels to enhance their cybersecurity awareness. The employed user's category receives specialized content focusing on cybersecurity in the workplace, addressing the critical need for professional and personal cybersecurity awareness. This personalized approach within the App ensures that each user receives an educational experience that aligns with their developmental stage or professional requirements.


Figure 28: “My Learning” Pages (Users Under 18 in the Middle, Above 18 in the Right)

#### *7.2.2.1 Users Aged under 18*

##### *7.2.2.1.1 Users Under 14 (School Students)*

School students under the age of 14 will be offered a course on cybersecurity awareness, concepts, and best practices, which are stratified into beginner, intermediate, and advanced levels. This content is delivered through interactive and captivating formats to engage students and enhance their understanding of cybersecurity.

*7.2.2.1.2 Users Between 14 and 18 (High School Students)*

The App provides advanced cybersecurity content for high school students between 14 and 18 years old. This content is an extension of the material provided to the under-14 category age group, but it is tailored to deepen their knowledge of cybersecurity concepts. The App engages students through interactive content, including thought-provoking videos and challenging scenarios designed to provoke critical thinking and reflection on cybersecurity best practices. The App also includes comprehensive quizzes to identify secure online behaviours and relatable stories that weave cybersecurity concepts together. Although the foundational topics are similar to those aimed at younger users, the approach is elevated to match high school students' advanced understanding and cognitive abilities.

*7.2.2.1.3 Content and Activities*

*7.2.2.1.3.1 Videos*

The videos in the application are animated and narrated with a tone that appeals to a younger audience, making them both educational and enjoyable. They are tailored to match the viewers' age and comprehension abilities. After watching the video, users are encouraged to test their grasp of the subject matter by completing a quiz. This interactive quiz feature not only assesses their understanding but also helps cement the information presented in the video, enhancing the learning experience. Figure 29 is an example of video content.

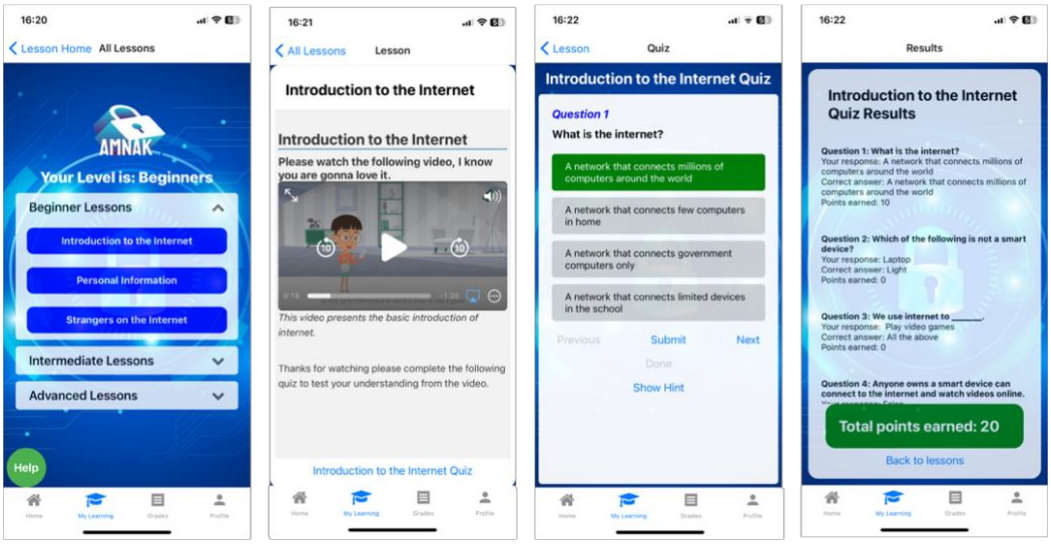



Figure 29: Example of Video Content for Users Under the Age of 18

*7.2.2.1.3.2 Stories*

The stories within the App are crafted to engage young learners by integrating cybersecurity principles into engaging tales. After reading the stories, students are prompted to articulate their takeaways by listing what they have learned. This activity not only reinforces their understanding but also encourages active reflection. Based on their answer input, the App provides feedback, validating correct observations and offering additional insights to ensure comprehensive learning. This interactive approach helps solidify the cybersecurity concepts presented in the story. Figure 30 is an example of story content.

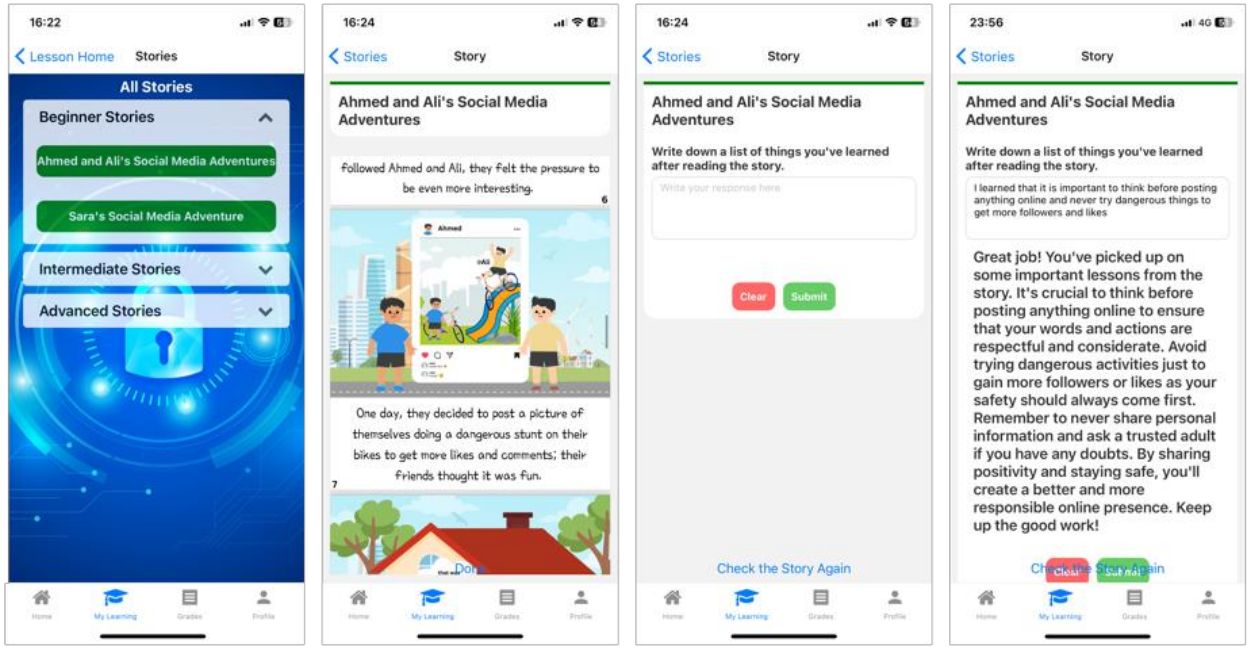



Figure 30: Example of Story Content for Users Under the Age of 18

*7.2.2.1.3.3 Scenarios*

The scenarios section of the App places students in real-life situations they might encounter online, prompting them to make decisions through multiple-choice questions. Once a selection is made, the App immediately provides feedback, indicating whether their choice was correct and explaining the rationale behind the correct response. This interactive feature helps students learn the importance of following the best practices through decision-making exercises. Figure 31 illustrates an example of scenario content provided for users under the age of 14 and between 14 and 18.

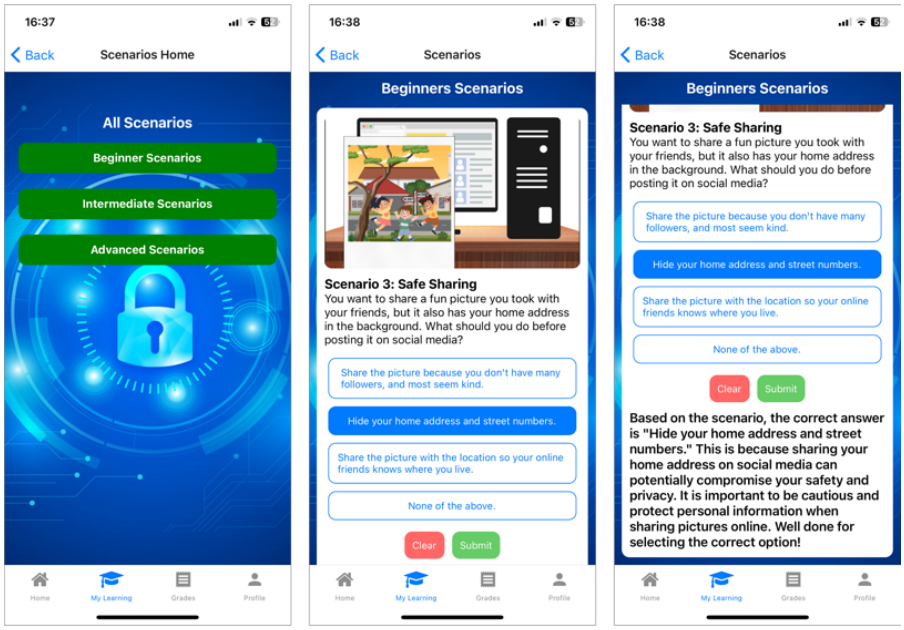



Figure 31: Example of Scenario Content for Users Under the Age of 18

### *7.2.2.2 Users Aged above 18*

#### *7.2.2.2.1 University Students, Graduates, Unemployed*

The application provides structured content of cybersecurity lessons tailored for individuals over the age of 18, including university students, graduates, or the unemployed. The content is systematically organized into beginners, intermediates, and advanced levels to cater to learners at different stages of their cybersecurity education.

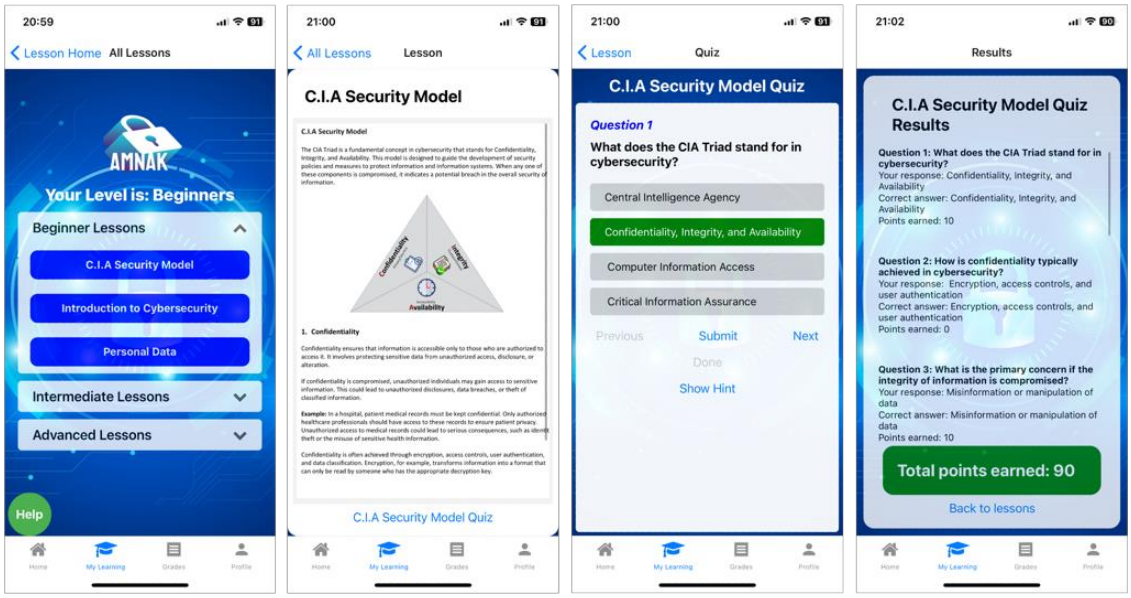



Figure 32: Example of Lesson Content for Users Above the Age of 18

Starting with the basics, users are introduced to the fundamental concepts and principles of cybersecurity, progressing through a series of topics that grow in complexity. As learners advance, they delve into intricate subjects such as malware, the nuances of social engineering attacks, and strategies to counteract various cyber threats. Each lesson culminates in an interactive quiz that reinforces the content learned and evaluates the user's understanding. Quiz results are immediately provided, giving valuable feedback that allows users to gauge their competency in each topic and identify areas needing additional focus, thus facilitating a complete and effective educational experience in cybersecurity.

*7.2.2.2.2 Employees*

The application offers cybersecurity lessons specifically designed for employees, targeting the critical awareness needed to protect sensitive data in today's organizational landscape. These lessons cover contemporary issues such as AI-driven scams, providing employees with the knowledge to identify and mitigate such threats. Upon completing a lesson, employees are presented with multiple-choice questions that evaluate their understanding of the subject matter. The quiz results provide immediate feedback, allowing for a clear assessment of their learning progress and ensuring they have grasped essential cybersecurity concepts critical for protecting their organization's digital assets. Figure 33 presents an example of a lesson content provided to employees.

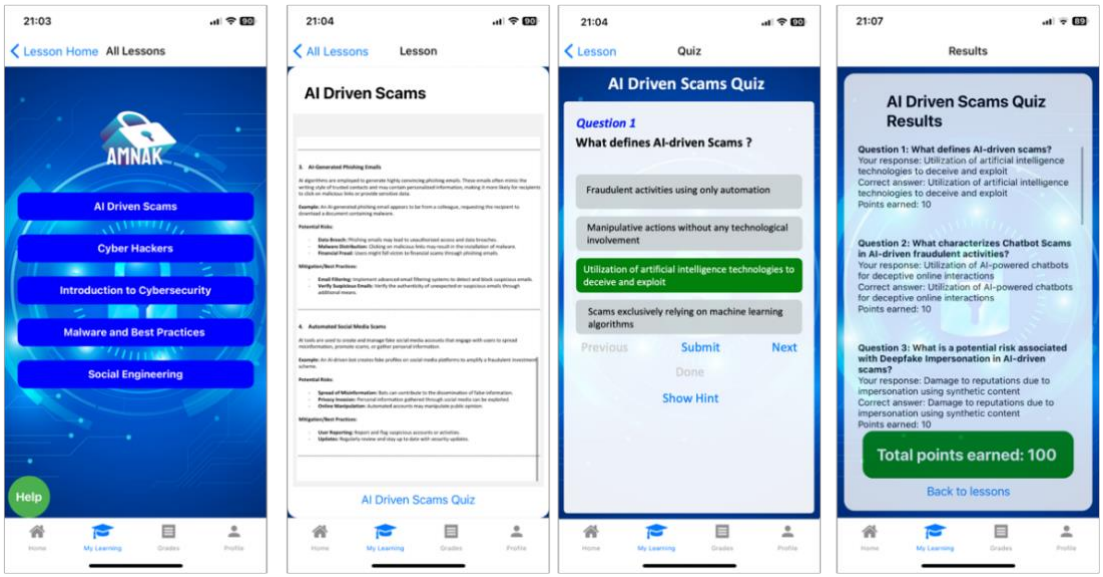



Figure 33: Example of Lesson Content for Employee Users

### *7.2.3 Evaluation Tests and Grades*

Users across all categories—under 14, ages 14 to 18, above 18, and employees—can access tailored evaluation tests within the application, designed to gauge their understanding of cybersecurity. These tests allow for multiple attempts and can be taken anytime, providing flexibility and continuous learning opportunities. Results from each attempt are recorded and displayed on the user's grades page, ensuring a clear view of progress and areas for improvement. The App generates 15 random multiple-choice questions for each evaluation from a comprehensive question bank that spans the content specific to each user category, ensuring a broad assessment, as shown in Figure 34.

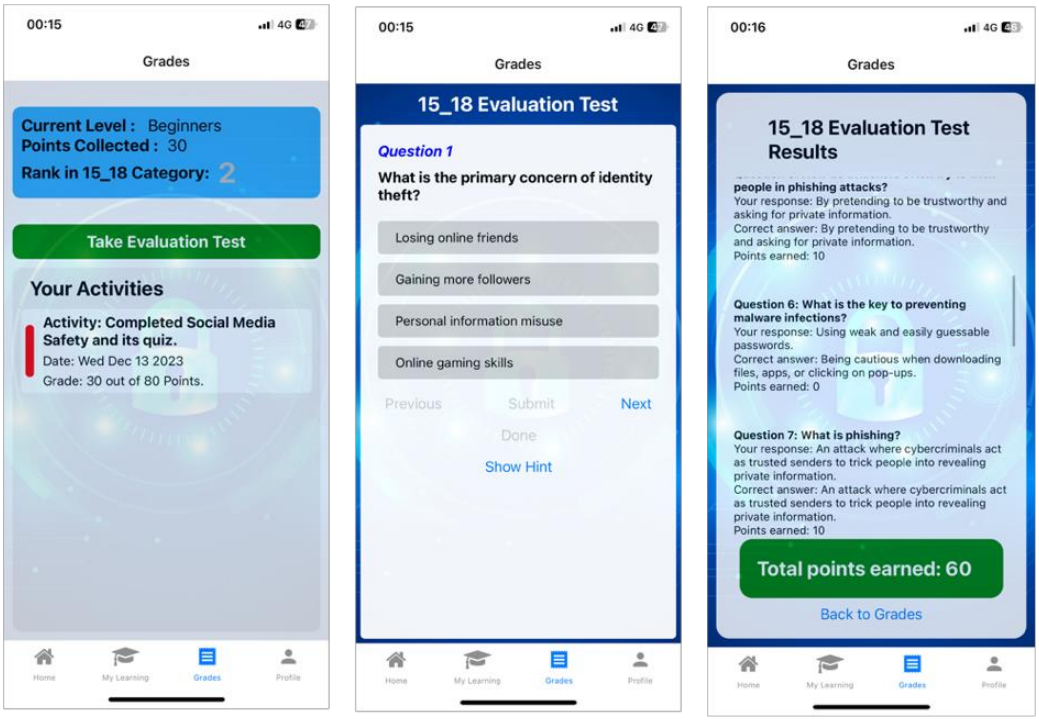



Figure 34: Evaluation Tests and Grades

### *7.2.4 Home Page Features*

The application’s home page presents a range of features that cater to users across all categories—under 14, 14 to 18, above 18, and employees. Alongside the "My Learning" component, which delivers age and role-specific content, the App provides universally accessible tools. These include "Cyber Security News," a "Cyber Security Certifications Roadmap," "Social Media Tips and Recommendations" related to privacy

and security, and "Report Cybercrimes," where users will be directed to concerned authorities. This layout ensures that users from any category can easily navigate and utilize the resources tailored to enhance their cybersecurity knowledge and skills.

### *7.2.4.1 Security News*

The application features a dedicated section for recent cybersecurity news, keeping users informed about the latest developments and threats in the field of cybersecurity. This section not only highlights important news events but also directs users to the original sources for in-depth reading. This functionality emphasizes the App's role as an educational tool, ensuring that users are not only learning about cybersecurity practices but are also aware of real-world applications and incidents.

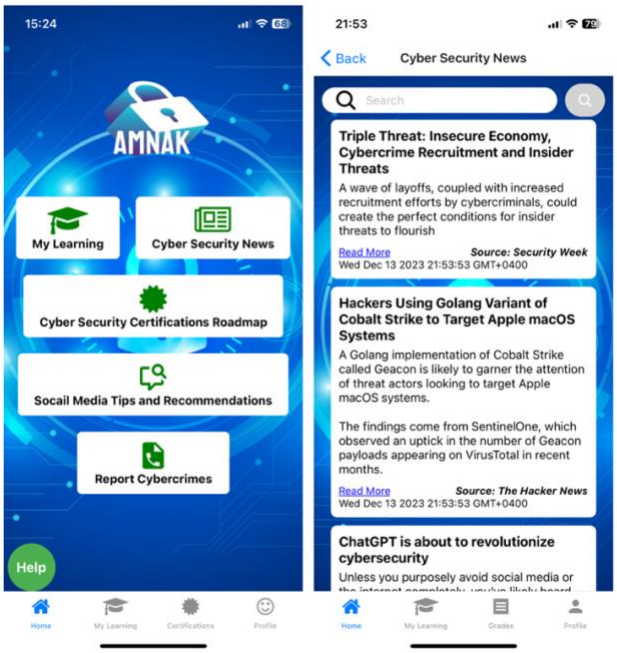



Figure 35: Security News Page

### *7.2.4.2 Security Certifications Roadmap*

The application presents a systematically organized and updated security certification roadmap presented in Figure 36 inspired by [164] tailored for IT and cybersecurity professionals. It categorizes certifications according to experience levels, directing users towards the most appropriate credentials for their career goals. The roadmap prioritizes obtaining relevant certifications over numerous others, aligning with

the National Initiative for Cybersecurity Careers and Studies (NICCS) standards to offer a defined path for professional growth and advancement in the industry.

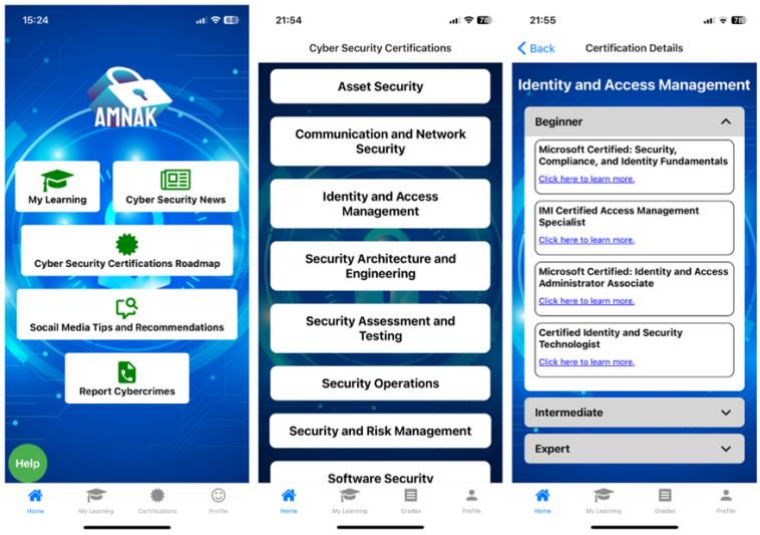



Figure 36: Security Certifications Roadmap

### *7.2.4.3 Report Cybercrimes*

The application has a helpful feature for users who want to report cybercrimes but are unsure of the appropriate channel. The App provides direct links to the official websites of the relevant authorities, enabling users to communicate their cybersecurity concerns promptly and securely to the proper channels as shown in Figure 37.

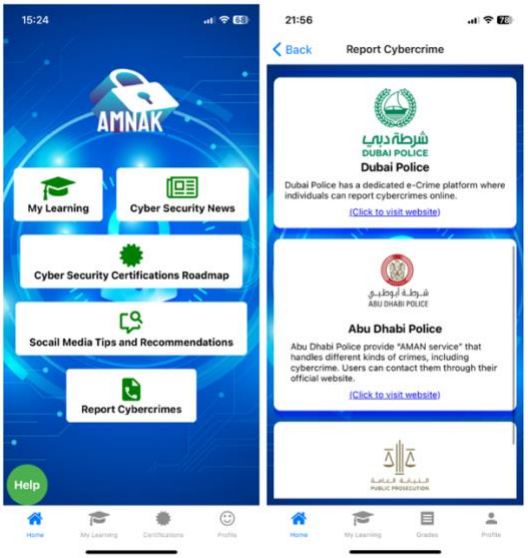



Figure 37: Report Cybercrimes Page

*7.2.4.4 Social Media Privacy and Security (Tips and Recommendations)*

The application furnishes users with essential security and privacy tips for social media, complemented by step-by-step instructions to make the process easier to navigate as shown in Figure 38. This feature is designed to help users enhance their digital safety and privacy on various platforms by walking them through recommended security measures.

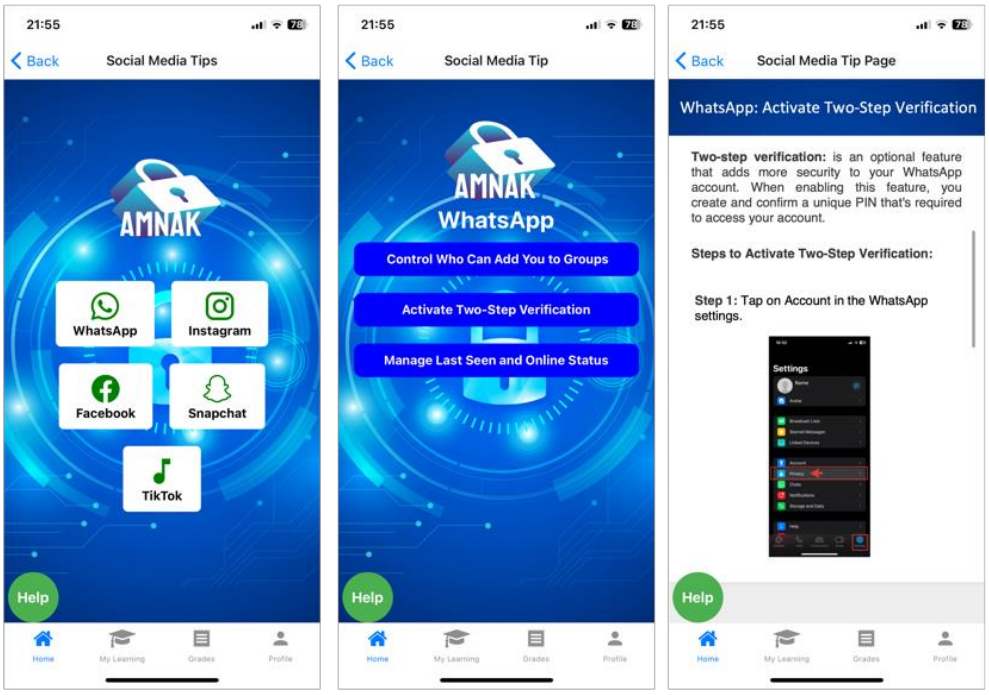



Figure 38: Social Media Privacy and Security

*7.2.4 AI Assistant*

In the application, GPT Turbo 3.5 serves both as a virtual customer service assistant and as a mechanism for delivering feedback and grades on user activities. It utilizes prepared prompts and dynamically generates responses to user inquiries or details about completed exercises, which are processed through the GPT API. GPT Turbo 3.5 leverages its advanced NLP capabilities to understand the queries and provide apt responses. As a virtual customer service assistant, it helps users by answering questions and offering necessary information. In terms of exercises, the API assesses users' submissions and provides feedback, integrating intelligent automation into the app's engagement and support functions. This dual role of GPT Turbo 3.5 significantly enriches the user

experience by facilitating personalized and contextually appropriate interactions within the application. Figure 39 presents a response to “What is malware?” from the Help Assistant in the app, and another example is the responses in the activities provided to users, such as Figure 30 and Figure 31.

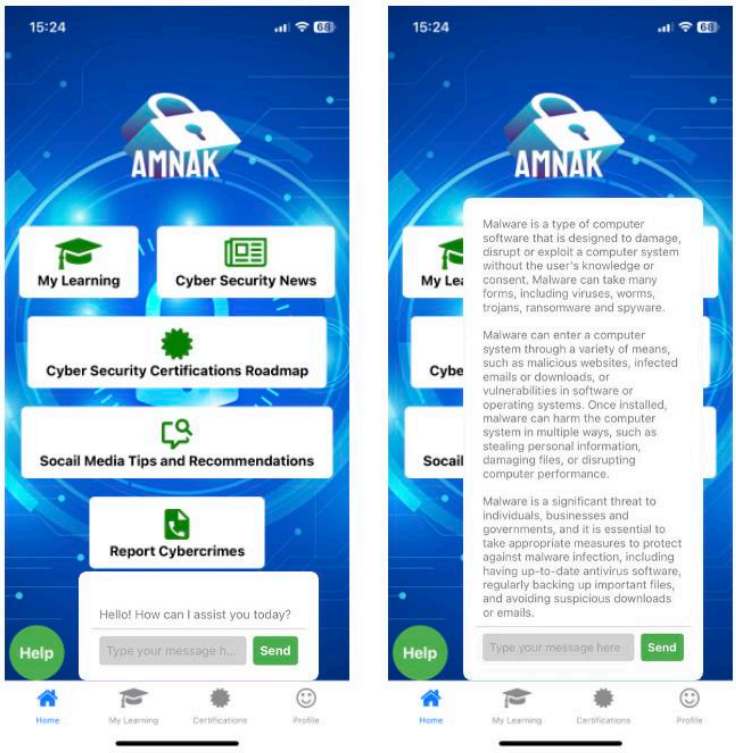



Figure 39: GPT-API Integration

## 7.3 System Design

### *7.3.1 Front-End Development*

The mobile application's front end is engineered using the React Native framework. This popular open-source framework supports the development of cross-platform applications, ensuring a unified and consistent user experience across iOS and Android devices. React Native harnesses React's capabilities to facilitate the construction of reusable UI components, streamlining both the development and ongoing maintenance processes. The mobile application's User Interface (UI) design is both intuitive and user-friendly. It follows a minimalist approach, focusing on ease of navigation and accessibility of features, making the application straightforward for users. The UI's responsive design adapts seamlessly to different screen sizes and orientations, providing an optimal

experience on a broad spectrum of mobile devices. Furthermore, the mobile application enhances its security measures by integrating with Firebase Authentication. This integration enables a secure system for user account creation, login, and password recovery. Firebase Authentication offers a comprehensive and scalable identity management system, significantly bolstering the application's security framework and ensuring user data protection.

### *7.3.2 Back-End Development*

The mobile application's back end utilizes Firebase Cloud Firestore to store and manage text-based data. As a NoSQL document database, Cloud Firestore enables real-time data synchronization between the front end and back end, ensuring that users can always access the latest information. This capability supports efficient data querying and scalability, which are essential for a mobile application's evolving demands. Additionally, the mobile application employs Firebase Cloud Storage to manage multimedia content, including images and videos. This cloud-based storage solution facilitates the seamless upload, download, and handling of media files, providing reliable and scalable storage options. Integrating Firebase Cloud Storage is crucial for maintaining the integrity and accessibility of multimedia content within the application, allowing for smooth retrieval and display of media to enhance user engagement.

## 7.4 Testing

Continuous testing was carried out through the deployment of the app via TestFlight, allowing external users to install and utilize its features and provide feedback on its functionality. Additionally, internal testing was conducted by the application developers. The insights gained from both testing phases have been instrumental in the ongoing enhancement and upgrading of the app to ensure its effectiveness and user satisfaction.

# Chapter 8: Conclusion

## 8.1 Summary of the Key Findings

The exploration of cybersecurity education and awareness within the UAE identifies critical gaps and challenges in public school curricula, university programs, and general public awareness. Foundational cybersecurity knowledge is notably absent in educational curricula, leading to a widespread need for enhanced digital safety awareness and the development of practical skills through real-world simulations. Additionally, there is insufficient coverage of cyber ethics, legal frameworks, and advanced threats, leaving students and the public ill-prepared to tackle emerging cyber challenges, including AI-driven attacks. Overall, there is an urgent need for comprehensive educational reforms and initiatives to bridge these gaps, equipping individuals with the knowledge and skills necessary to navigate and secure their digital environments effectively. The development of the AI-enhanced mobile application, as detailed in Chapter 7, represents a significant stride towards bridging the cybersecurity awareness gap in the UAE. By tailoring content to specific age groups and professional backgrounds, the application ensures that users receive relevant, engaging, and practical cybersecurity education. The integration of AI, particularly through GPT Turbo 3.5, enhances the learning experience by providing personalized assistance and feedback, thereby fostering a deeper understanding of cybersecurity threats and best practices among users. The application's design, coupled with continuous testing and user feedback, underscores the commitment to creating a dynamic and effective educational tool. This initiative addresses the identified gaps in cybersecurity education and awareness and lays the groundwork for a more secure digital environment in the UAE.

## 8.2 Challenges and Limitations

The study and the development of the AI-enhanced mobile application faced several challenges and limitations that are important to acknowledge. Firstly, the content within the app, while comprehensive, is still limited and requires further expansion to cover the vast spectrum of cybersecurity topics and scenarios that users may encounter. Additionally, the survey conducted to assess cybersecurity awareness in the UAE involved 500 participants, a sample size that, although significant, may not fully represent the

diverse population of the UAE. This limitation suggests the need for broader studies to capture a more comprehensive understanding of cybersecurity awareness across different segments of the UAE population. In terms of curriculum gap analysis within schools, the review was specifically based on the 2023-2024 academic year and was restricted due to the unavailability of certain materials from Tawzea, a major organization specializing in integrated logistics services and the distributor of MoE school books [165]. Consequently, the analysis did not encompass Term 3 or the materials in Grades 9 to 12 in Term 1. This exclusion may have resulted in potential oversights regarding crucial aspects of cybersecurity education for these educational stages. For university program analysis, the examination was generalized and did not delve deeply into the specific courses learning outcomes of each program or their alignment with international standards, which could provide a more detailed understanding of where these programs stand compared to global benchmarks. Addressing these challenges and limitations in future iterations of the study and app development will be crucial for enhancing the effectiveness of cybersecurity education and awareness efforts in the UAE.

### 8.3 Future Research Directions

Future research directions from this study suggest a multifaceted approach to advancing cybersecurity education and awareness in the UAE. Firstly, considering the UAE's linguistic and cultural context, developing an Arabic version of the application is crucial. This adaptation would make the app more accessible to native Arabic speakers and ensure cybersecurity education is deeply integrated into the local context. Additionally, comprehensive software testing should be conducted to ensure the application's functionality, security, and user-friendliness. This testing will help identify and rectify potential issues before the app is widely deployed, enhancing the overall quality and effectiveness of the cybersecurity learning tool. Another important area for future work involves testing the application on a broader audience covering all age groups. This testing should assess their cybersecurity awareness levels at the onset of using the application and after engaging with it, utilizing the evaluation tests and quizzes embedded within the app. Such assessments will provide valuable insights into the educational impact of the application and highlight areas for further content refinement and user engagement strategies. Longitudinal studies could also be conducted to evaluate the long-

term impact of cybersecurity education reforms and the effectiveness of AI-enhanced learning tools in improving cybersecurity awareness and skills among various demographics. Investigating the scalability and adaptability of the developed mobile application across different cultures and educational systems would provide further insights into global cybersecurity education strategies. Further research might explore integrating emerging technologies such as augmented reality (AR) and virtual reality (VR) to create more immersive and interactive cybersecurity learning experiences. Additionally, studies focusing on the psychological and behavioral aspects of cybersecurity awareness could offer a deeper understanding of how individuals perceive and respond to cyber threats, guiding the development of more effective educational content and engagement strategies. Collaborative research involving academia, industry, and government agencies could yield comprehensive cybersecurity frameworks that address current and emerging threats while fostering a culture of cyber resilience. Lastly, exploring the pathways to more effectively aligning cybersecurity education with professional certification and industry standards could bridge the gap between academic preparation and professional requirements, enhancing the workforce readiness of cybersecurity graduates.

## References


[1] E. McCallister, T. Grance, and K. A. Scarfone, 'Guide to protecting the confidentiality of Personally Identifiable Information (PII)', Gaithersburg, MD, 2010. doi: 10.6028/NIST.SP.800-122.

[2] TDRA, 'National Cybersecurity Strategy', UAE. Accessed: Feb. 05, 2024. [Online]. Available: https://tdra.gov.ae/userfiles/assets/Lw3seRUaIMd.pdf

[3] The National News, 'UAE working on "GPT-powered AI tutors" to transform education'. Accessed: May 25, 2023. [Online]. Available: https://www.thenationalnews.com/uae/education/2023/03/04/uae-working-on-gpt-powered-ai-tutors-to-transform-education/

[4] F. Ouyang, M. Wu, L. Zheng, L. Zhang, and P. Jiao, 'Integration of artificial intelligence performance prediction and learning analytics to improve student learning in online engineering course', *International Journal of Educational Technology in Higher Education*, vol. 20, no. 1, Dec. 2023, doi: 10.1186/s41239-022-00372-4.

[5] National Program for Artificial Intelligence, 'Ministerial Forward Executive Summary', 2031. Accessed: Mar. 30, 2023. [Online]. Available: https://ai.gov.ae/wp-content/uploads/2021/07/UAE-National-Strategy-for-Artificial-Intelligence-2031.pdf

[6] National Program for Artificial Intelligence, 'AI Guide'. Accessed: Mar. 30, 2023. [Online]. Available: https://ai.gov.ae/wp-content/uploads/2020/02/AIGuide_EN_v1-online.pdf

[7] W. J. Triplett, 'Addressing Human Factors in Cybersecurity Leadership', *Journal of Cybersecurity and Privacy*, vol. 2, no. 3, pp. 573–586, Jul. 2022, doi: 10.3390/jcp2030029.

[8] Sophos, 'The State of Ransomware 2022', 2022. Accessed: Mar. 26, 2023. [Online]. Available: https://assets.sophos.com/X24WTUEQ/at/4zpw59pnkpxxnhfhgj9bxgj9/sophos-state-of-ransomware-2022-wp.pdf

[9] M. Harika and E. Campbell, 'Ransomware in the UAE: Evolving threats and expanding responses'. Accessed: Apr. 02, 2023. [Online]. Available: https://www.mei.edu/publications/ransomware-uae-evolving-threats-and-expanding-responses

[10] L. Li, W. He, L. Xu, I. Ash, M. Anwar, and X. Yuan, 'Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior', *Int J Inf Manage*, vol. 45, pp. 13–24, Apr. 2019, doi: 10.1016/j.ijinfomgt.2018.10.017.

[11] R. Sabillon, J. Serra-Ruiz, V. Cavaller, and J. Cano, ‘A comprehensive cybersecurity audit model to improve cybersecurity assurance: The cybersecurity audit model (CSAM)’, in *Proceedings - 2017 International Conference on Information Systems and Computer Science, INCISCOS 2017*, Institute of Electrical and Electronics Engineers Inc., Mar. 2018, pp. 253–259. doi: 10.1109/INCISCOS.2017.20.

[12] Y. Li and Q. Liu, ‘A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments’, *Energy Reports*, vol. 7, pp. 8176–8186, Nov. 2021, doi: 10.1016/j.egyr.2021.08.126.

[13] I. Emmanuel O, C. Ekele Victoria, I. Omonigho Efeoghene, and C. Nwachuwku Praise, ‘Overview of Recent Cyberattacks: A Systematic Review’, in *2023 International Conference on Science, Engineering and Business for Sustainable Development Goals, SEB-SDG 2023*, Institute of Electrical and Electronics Engineers Inc., 2023. doi: 10.1109/SEB-SDG57117.2023.10124473.

[14] M. Mijwil, O. J. Unogwu, Y. Filali, I. Bala, and H. Al-Shahwani, ‘Exploring the Top Five Evolving Threats in Cybersecurity: An In-Depth Overview’, *Mesopotamian Journal of Cyber Security*, pp. 57–63, Mar. 2023, doi: 10.58496/mjcs/2023/010.

[15] L. Peng and Q. Lemke, ‘Research trends in cybercrime and cybersecurity: A review based on Web of Science core collection database’, 2023. Accessed: May. 27, 2023. [Online]. Available: https://vc.bridgew.edu/ijcic

[16] FBI, ‘2022 Internet Crime Report’, 2022. Accessed: May 27, 2023. [Online]. Available: https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf

[17] FBI, ‘2020 Internet Crime Report’. Accessed: May 27, 2023. [Online]. Available: https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

[18] S. Chng, H. Y. Lu, A. Kumar, and D. Yau, ‘Hacker types, motivations and strategies: A comprehensive framework’, *Computers in Human Behavior Reports*, vol. 5. Elsevier Ltd, Mar. 01, 2022. doi: 10.1016/j.chbr.2022.100167.

[19] Dr. A. Marelino, ‘Understanding the Types of Cyber Crime and Its Prevention’, *Mathematical Statistician and Engineering Applications*, vol. 71, no. 1, Jan. 2022, doi: 10.17762/msea.v71i1.50.

[20] S. L. N. Hald and J. M. Pedersen, ‘An Updated Taxonomy for Characterizing Hackers According to Their Threat Properties’, in *14th International Conference on Advanced Communication Technology (ICACT)*, IEEE, 2012, pp. 81–86.

[21] C. Moeckel, ‘Examining and constructing attacker categorisations — An experimental typology for digital banking’, in *ACM International Conference Proceeding Series*, Association for Computing Machinery, Aug. 2019. doi: 10.1145/3339252.3340341.

[22] S. Atkinson and C. Walker, ‘sans-psychology-and-the-hacker-psychological-incident-handling’, *The SANS Institute*, Jun. 2015, Accessed: Jan. 22, 2024. [Online]. Available: https://sansorg.egnyte.com/dl/qujoT8yBc8

[23] J. Gaia, G. Lawrence Sanders, S. Patrick Sanders, X. Wang, and C. Woo Yoo, ‘Dark Traits and Hacking Potential’, *J Organ Psychol*, vol. 21, no. 3, p. 23, 2021, Accessed: Jan. 22, 2024. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3888759

[24] M. N. Al Mhiqani *et al.*, ‘A new taxonomy of insider threats: an initial step in understanding authorised attack’, *International Journal of Information Systems and Management*, vol. 1, no. 4, p. 343, 2018, doi: 10.1504/ijisam.2018.094777.

[25] I. C. Eian, K. Y. Lim, M. X. L. Yeap, H. Q. Yeo, and F. Z, ‘Wireless Networks: Active and Passive Attack Vulnerabilities and Privacy Challenges’, *Preprints (Basel)*, Oct. 2020, doi: 10.20944/PREPRINTS202010.0018.V1.

[26] A. Qamar, A. Karim, and V. Chang, ‘Mobile malware attacks: Review, taxonomy & future directions’, *Future Generation Computer Systems*, vol. 97, pp. 887–909, Aug. 2019, doi: 10.1016/J.FUTURE.2019.03.007.

[27] H. Deylami, R. Chandren Muniyandi, I. T. Ardekani, and A. Sarrafzadeh, ‘Taxonomy of Malware Detection Techniques: A Systematic Literature Review’, in *2016 14th Annual Conference on Privacy, Security and Trust (PST)*, 2016, pp. 629–636. doi: 10.1109/PST.2016.7906998.

[28] D.-L. Copaci and C.-A. Copaci, ‘Types of Attacks and Security Methods. Virtual Machines’, *Proceedings of the International Conference on Cybersecurity and Cybercrime*, pp. 135–140, May 2023.

[29] A. Farion-Melnyk, V. Rozheliuk, T. Slipchenko, S. Banakh, M. Farion, and O. Bilan, ‘Ransomware Attacks: Risks, Protection and Prevention Measures’, in *2021 11th International Conference on Advanced Computer Information Technologies, ACIT 2021 - Proceedings*, Institute of Electrical and Electronics Engineers Inc., Sep. 2021, pp. 473–478. doi: 10.1109/ACIT52158.2021.9548507.

[30] J. Gao, L. Li, P. Kong, T. F. Bissyandé, and J. Klein, ‘Should You Consider Adware as Malware in Your Study?’, in *IEEE 26th International Conference on Software Analysis, Evolution and Reengineering (SANER)*, 2019, pp. 604–608. doi: 10.1109/SANER.2019.8668010.

[31] F. Salahdine and N. Kaabouch, ‘Social engineering attacks: A survey’, *Future Internet*, vol. 11, no. 4. MDPI AG, 2019. doi: 10.3390/FI11040089.

[32] N. Pilavakis, A. Jenkins, N. Kökciyan, and K. Vaniea, ‘“I didn’t click”: What users say when reporting phishing’, in *Proceedings 2023 Symposium on Usable Security*, Reston, VA: Internet Society, 2023. doi: 10.14722/usec.2023.233129.

[33] Z. Wang, L. Sun, and H. Zhu, ‘Defining Social Engineering in Cybersecurity’, *IEEE Access*, vol. 8, pp. 85094–85115, 2020, doi: 10.1109/ACCESS.2020.2992807.

[34] A. Kamruzzaman, K. Thakur, S. Ismat, M. L. Ali, K. Huang, and H. N. Thakur, ‘Social Engineering Incidents and Preventions’, in *2023 IEEE 13th Annual Computing and Communication Workshop and Conference, CCWC 2023*, Institute of Electrical and Electronics Engineers Inc., 2023, pp. 494–498. doi: 10.1109/CCWC57344.2023.10099202.

[35] F. Yihunie, E. Abdelfattah, and A. Odeh, ‘Analysis of ping of death DoS and DDoS attacks’, in *2018 IEEE Long Island Systems, Applications and Technology Conference (LISAT)*, 2018, pp. 1–4. doi: 10.1109/LISAT.2018.8378010.

[36] G. Anand, S. B. Prathiba, Gunasekaran, and Ponmani, ‘Detection of Man In The Middle Attacks in Wi-Fi networks by IP Spoofing’, in *2018 Tenth International Conference on Advanced Computing (ICoAC)*, 2018, pp. 319–322. doi: 10.1109/ICoAC44903.2018.8939063.

[37] E. Letsoalo and S. Ojo, ‘A Model to Mitigate Session Hijacking Attacks in Wireless Networks’, in *2018 IST-Africa Week Conference (IST-Africa)*, 2018, p. Page 1 of 10-Page 10 of 10.

[38] A. A. Alghamdi, ‘Overview of Cybersecurity Challenges in Fourth Industrial Revolution’, *Turkish Journal of Computer and Mathematics Education*, vol. 12, no. 7, pp. 565–570, 2021, Accessed: Jan. 24, 2024. [Online]. Available: https://www.turcomat.org/index.php/turkbilmat/article/view/2623

[39] G. Buah, S. Memusi, J. Munyi, T. Brown, and R. A. Sowah, ‘Vulnerability Analysis of Online Banking Sites to Cross-Site Scripting and Request Forgery Attacks: A Case Study in East Africa’, in *IEEE International Conference on Adaptive Science and Technology, ICAST*, IEEE Computer Society, 2021. doi: 10.1109/ICAST52759.2021.9681978.

[40] B. Guembe, A. Azeta, S. Misra, V. C. Osamor, L. Fernandez-Sanz, and V. Pospelova, ‘The Emerging Threat of Ai-driven Cyber Attacks: A Review’, *Applied Artificial Intelligence*, vol. 36, no. 1. Taylor and Francis Ltd., 2022. doi: 10.1080/08839514.2022.2037254.

[41] M. M. Yamin, M. Ullah, H. Ullah, and B. Katt, ‘Weaponized AI for cyber attacks’, *Journal of Information Security and Applications*, vol. 57, Mar. 2021, doi: 10.1016/j.jisa.2020.102722.

[42] S. M. Hassan and J. Wasim, ‘Study of Artificial Intelligence in Cyber Security And The Emerging Threat of AI-Driven Cyber Attacks and Challenge’, *Journal of Aeronautical Materials* , vol. 43, no. 1, pp. 1557–1570, 2023, Accessed: Jan. 24, 2024. [Online]. Available: https://ssrn.com/abstract=4652028

[43] N. H. Al-Kumaim and S. K. Alshamsi, ‘Determinants of Cyberattack Prevention in UAE Financial Organizations: Assessing the Mediating Role of Cybersecurity Leadership’, *Applied Sciences*, vol. 13, no. 10, p. 5839, May 2023, doi: 10.3390/app13105839.

[44] SOCRadar, ‘UNITED ARAB EMIRATES Threat Landscape Report’, 2022. Accessed: Jan. 25, 2024. [Online]. Available: https://socradar.io/wp-content/uploads/2022/11/UAE-Threat-Landscape-Report.pdf

[45] AECERT, ‘INCIDENTS WE DEALT WITH, Monthly UAE report on information security subjects’, United Arab Emirates, Dec. 2019. Accessed: Jan. 25, 2024. [Online]. Available: https://tdra.gov.ae/userfiles/assets/POUfF6ZqdSp.pdf

[46] W. Mercer and P. Rascagnères, ‘DNS ON FIRE’, *Virus Bulletin*, London, Oct. 2019. Accessed: Jan. 25, 2024. [Online]. Available: https://www.virusbulletin.com/uploads/pdf/magazine/2019/VB2019-Mercer-Rascagneres.pdf

[47] AECERT, ‘Updated Shamoon Malware Profile Security Advisory Criticality’, United Arab Emirates, Jan. 2017. Accessed: Jan. 25, 2024. [Online]. Available: https://tdra.gov.ae/userfiles/assets/MOUmUDpb61R.pdf

[48] M. N. Al-Mhiqani *et al.*, ‘Cyber-Security Incidents: A Review Cases in Cyber-Physical Systems’, *IJACSA) International Journal of Advanced Computer Science and Applications*, vol. 9, no. 1, pp. 499–508, 2018, doi: 10.14569/IJACSA.2018.090169.

[49] A. Drozhzhin, ‘Adwind malware-as-a-service hits more than 400,000 users globally’. Accessed: Jan. 24, 2024. [Online]. Available: https://www.kaspersky.com/blog/adwind-rat/11252/

[50] M. Zwilling, G. Klien, D. Lesjak, Ł. Wiechetek, F. Cetin, and H. N. Basim, ‘Cyber Security Awareness, Knowledge and Behavior: A Comparative Study’, *Journal of Computer Information Systems*, vol. 62, no. 1, pp. 82–97, 2022, doi: 10.1080/08874417.2020.1712269.

[51] Y. K. Peker, L. Ray, and S. Da Silva, ‘Online cybersecurity awareness modules for college and high school students’, in *Proceedings - 2018 National Cyber Summit Research Track, NCS 2018*, Institute of Electrical and Electronics Engineers Inc., Dec. 2018, pp. 24–33. doi: 10.1109/NCS.2018.00009.

[52] F. Quayyum, D. S. Cruzes, and L. Jaccheri, ‘Cybersecurity awareness for children: A systematic literature review’, *International Journal of Child-Computer Interaction*, vol. 30. Elsevier B.V., Dec. 01, 2021. doi: 10.1016/j.ijcci.2021.100343.

[53] S. S. Tirumala, A. Sarrafzadeh, and P. Pang, ‘A survey on Internet usage and cybersecurity awareness in students’, 2016.

[54] M. A. Alqahtani, ‘Factors Affecting Cybersecurity Awareness among University Students’, *Applied Sciences (Switzerland)*, vol. 12, no. 5, Mar. 2022, doi: 10.3390/app12052589.

[55] M. Khader, M. Karam, and H. Fares, ‘Cybersecurity awareness framework for academia’, *Information (Switzerland)*, vol. 12, no. 10, Oct. 2021, doi: 10.3390/info12100417.

[56] R. Ismailova and G. Muhametjanova, ‘Cyber crime risk awareness in Kyrgyz Republic’, *Information Security Journal*, vol. 25, no. 1–3, pp. 32–38, Apr. 2016, doi: 10.1080/19393555.2015.1132800.

[57] N. Ahmed, U. Kulsum, I. Bin Azad, A. S. Z. Momtaz, M. E. Haque, and M. S. Rahman, ‘Cybersecurity awareness survey: An analysis from Bangladesh perspective’, in *2017 IEEE Region 10 Humanitarian Technology Conference (R10-HTC)*, 2017, pp. 788–791. doi: 10.1109/R10-HTC.2017.8289074.

[58] G. H. Kirwan, C. Fullwood, and B. Rooney, ‘Risk Factors for Social Networking Site Scam Victimization Among Malaysian Students’, *Cyberpsychol Behav Soc Netw*, vol. 21, no. 2, pp. 123–128, 2018, doi: 10.1089/cyber.2016.0714.

[59] A. A. Garba, M. M. Siraj, S. H. Othman, and M. A. Musa, ‘A Study on Cybersecurity Awareness Among Students in Yobe State University, Nigeria: A Quantitative Approach’, *International Journal on Emerging Technologies*, vol. 11, no. 5, pp. 41–49, 2020, Accessed: Jan. 27, 2024. [Online]. Available: www.researchtrend.net

[60] A. A. Al Shamsi, ‘Effectiveness of Cyber Security Awareness Program for young children: A Case Study in UAE’, *International Journal of Information Technology and Language Studies (IJITLS)*, vol. 3, no. 2, pp. 8–29, 2019, doi: 10.13140/RG.2.2.28488.14083.

[61] F. A. Aloul, ‘The Need for Effective Information Security Awareness’, *Journal of Advances in Information Technology*, vol. 3, no. 3, Aug. 2012, doi: 10.4304/jait.3.3.176-183.

[62] S. Maisikeli, ‘UAE Cybersecurity Perception and Risk Assessments Compared to Other Developed Nations’, in *2020 3rd International Conference on Information and Computer Technologies (ICICT)*, 2020, pp. 432–439. doi: 10.1109/ICICT50521.2020.00075.

[63] O. Sirajeldeen Ahmed, S. Ameen Nasef, A. Zuhir Al Rawashdeh, and M. Elmagzoub Eltahir, ‘Teacher’s awareness to develop student cyber security: A Case Study’, *Turkish Journal of Computer and Mathematics Education*, vol. 12, no. 10, pp. 5148–5156, 2021, doi: https://doi.org/10.17762/turcomat.v12i10.5297.

[64] P. Flores, M. Farid, and K. Samara, ‘Assessing E-Security Behavior among Students in Higher Education’, in *2019 Sixth HCT Information Technology Trends (ITT)*, 2019, pp. 253–258. doi: 10.1109/ITT48889.2019.9075100.

[65] F. Alotaibi, S. Furnell, I. Stengel, and M. Papadaki, ‘A Review of Using Gaming Technology for Cyber-Security Awareness’, *International Journal for Information Security Research (IJISR)*, vol. 6, no. 2, pp. 660–666, 2016, Accessed: Feb. 01, 2024. [Online]. Available: https://infonomics-society.org/wp-content/uploads/ijisr/published-papers/volume-6-2016/A-Review-of-Using-Gaming-Technology-for-Cyber-Security-Awareness.pdf

[66] F. Alotaibi, S. Furnell, I. Stengel, and M. Papadaki, ‘Enhancing cyber security awareness with mobile games’, in *2017 12th International Conference for Internet Technology and Secured Transactions (ICITST)*, 2017, pp. 129–134. doi: 10.23919/ICITST.2017.8356361.

[67] H. Qusa and J. Tarazi, ‘Cyber-Hero: A Gamification framework for Cyber Security Awareness for High Schools Students’, in *2021 IEEE 11th Annual Computing and Communication Workshop and Conference, CCWC 2021*, Institute of Electrical and Electronics Engineers Inc., Jan. 2021, pp. 677–682. doi: 10.1109/CCWC51732.2021.9375847.

[68] F. Abu-Amara, R. Almansoori, S. Alharbi, M. Alharbi, and A. Alshehhi, ‘A novel SETA-based gamification framework to raise cybersecurity awareness’, *International Journal of Information Technology*, vol. 13, no. 6, pp. 2371–2380, 2021, doi: 10.1007/s41870-021-00760-5.

[69] E. Löffler, B. Schneider, P. M. Asprion, and T. Zanwar, ‘CySecEscape 2.0-A virtual escape room to raise cybersecurity awareness’, *International Journal of Serious Games*, vol. 8, no. 1, pp. 59–70, 2021, doi: 10.17083/ijsg.v8i1.413.

[70] S. Hart, A. Margheri, F. Paci, and V. Sassone, ‘Riskio: A Serious Game for Cyber Security Awareness and Education’, *Comput Secur*, vol. 95, Aug. 2020, doi: 10.1016/j.cose.2020.101827.

[71] H. Alqahtani and M. Kavakli-Thorne, ‘Design and evaluation of an augmented reality game for cybersecurity awareness (CybAR)’, *Information (Switzerland)*, vol. 11, no. 2, Feb. 2020, doi: 10.3390/info11020121.

[72] J. Pérez, R. Torres, and S. von Brand, ‘CyberKids: video game for raising cyber security awareness in children’, in *2020 39th International Conference of the Chilean Computer Science Society (SCCC)*, 2020, pp. 1–8. doi: 10.1109/SCCC51225.2020.9281253.

[73] L. A. Scholefield Sam and Shepherd, ‘Gamification Techniques for Raising Cyber Security Awareness’, in *HCI for Cybersecurity, Privacy and Trust*, A. Moallem, Ed., Cham: Springer International Publishing, 2019, pp. 191–203.

[74] A. Yasin, L. Liu, T. Li, R. Fatima, and W. Jianmin, ‘Improving software security awareness using a serious game’, *IET Software*, vol. 13, no. 2, pp. 159–169, Apr. 2019, doi: 10.1049/iet-sen.2018.5095.

[75] A. Yasin, L. Liu, T. Li, J. Wang, and D. Zowghi, ‘Design and preliminary evaluation of a cyber Security Requirements Education Game (SREG)’, *Inf Softw Technol*, vol. 95, pp. 179–200, Mar. 2018, doi: 10.1016/j.infsof.2017.12.002.

[76] V. Lombardi, S. Ortiz, J. Phifer, T. Cerny, and D. Shin, ‘Behavior control-based approach to influencing user’s cybersecurity actions using mobile news app’, in *Proceedings of the ACM Symposium on Applied Computing*, Association for Computing Machinery, Mar. 2021, pp. 912–915. doi: 10.1145/3412841.3442103.

[77] A. M. Jafri, N. Z. Jamaluddin, and Z. Zulkifli, ‘Cybersecurity awareness mobile apps for secondary school students: LetSecure’, *Journal of Information Systems and Digital Technologies*, vol. 3, no. 2, pp. 94–108, Sep. 2021, Accessed: Feb. 7, 2024. [Online]. Available: https://journals.iium.edu.my/kict/index.php/jisdt/article/view/240

[78] H. M. Jawad and S. Tout, ‘Introducing a Mobile App to Increase Cybersecurity Awareness in MENA’, in *2020 3rd International Conference on Signal Processing and Information Security (ICSPIS)*, 2020, pp. 1–4. doi: 10.1109/ICSPIS51252.2020.9340128.

[79] D. Mhlanga, ‘Open AI in Education, the Responsible and Ethical Use of ChatGPT Towards Lifelong Learning’, 2023. Accessed: Feb. 13, 2024. [Online]. Available: https://ssrn.com/abstract=4354422

[80] I. Syamsuddin, R. Nur, Irmawati, K. Kasim, M. F. Raharjo, and K. Muchtar, ‘Evaluation of CyPACH: A Cyber Privacy Advisor Chatbot’, in *2023 2nd International Conference on Computer System, Information Technology, and Electrical Engineering (COSITE)*, 2023, pp. 7–12. doi: 10.1109/COSITE60233.2023.10249650.

[81] E. M. Dillon, C. Carpenter, J. Cook, T. D. Wills, and H. S. Narman, ‘A Machine Learning-Based Automatic Feedback System to Teach Cybersecurity Principles to K-12 and College Students’, in *2022 IEEE Global Humanitarian Technology Conference, GHTC 2022*, Institute of Electrical and Electronics Engineers Inc., 2022, pp. 219–225. doi: 10.1109/GHTC55712.2022.9910998.

[82] M. Hijji and G. Alam, ‘Cybersecurity Awareness and Training (CAT) Framework for Remote Working Employees’, *Sensors*, vol. 22, no. 22, Nov. 2022, doi: 10.3390/s22228663.

[83] T. Espinha Gasiba, U. Lechner, and M. Pinto-Albuquerque, ‘Sifu - a cybersecurity awareness platform with challenge assessment and intelligent coach’, *Cybersecurity*, vol. 3, no. 1, Dec. 2020, doi: 10.1186/s42400-020-00064-4.

[84] Ministry of Education - UAE, ‘About the Ministry’. Accessed: Feb. 21, 2024. [Online]. Available: https://www.moe.gov.ae/En/AboutTheMinistry/Pages/About.aspx

[85] Ministry of Education - UAE, ‘MOE Strategy’. Accessed: Feb. 21, 2024. [Online]. Available: https://www.moe.gov.ae/En/AboutTheMinistry/Pages/VisionMission.aspx

[86] The United Arab Emirates’ Government portal, ‘Stages and Streams of School Education’. Accessed: Feb. 21, 2024. [Online]. Available: https://u.ae/en/information-and-services/education/school-education-k-12/joining-k-12-education/stages-and-streams-of-school-education

[87] Ministry of Education - UAE, ‘Education today, for a reimagined tomorrow’. Accessed: Feb. 21, 2024. [Online]. Available: https://www.moe.gov.ae/en/pages/home.aspx

[88] A. Elnagar and M. Ghazal, ‘AI in the United Arab Emirates’ computing, creative design and innovation K-12 curriculum A case study’, UNESCO, 2024, pp. 1–70. Accessed: Feb. 21, 2024. [Online]. Available: https://unesdoc.unesco.org/ark:/48223/pf0000388652

[89] Ministry of Education - UAE, *Computing, Creative, Design & Innovation, Student Book (Course Book), Cycle 01, Grade 3*, vol. 1. 2023-2024.

[90] Ministry of Education - UAE, *Computing, Creative, Design & Innovation, Activity Book (Workbook), Cycle 01, Grade 3*, vol. 1. 2023-2024.

[91] Ministry of Education - UAE, *Computing, Creative, Design & Innovation, Student Book (Course Book), Cycle 01, Grade 4*, vol. 1. 2023-2024.

[92] Ministry of Education - UAE, *Computing, Creative, Design & Innovation, Activity Book (Workbook), Cycle 01, Grade 4*, vol. 1. 2023-2024.

[93] Ministry of Education - UAE, *Computing, Creative, Design & Innovation, Student Book (Course Book), Cycle 01, Grade 1*, vol. 1. 2023-2024.

[94] Ministry of Education - UAE, *Computing, Creative, Design & Innovation, Activity Book (Workbook), Cycle 01, Grade 1*, vol. 1. 2023-2024.

[95] Ministry of Education - UAE, *Computing, Creative, Design & Innovation, Student Book (Course Book), Cycle 01, Grade 2*, vol. 1. 2023-2024.

[96] Ministry of Education - UAE, *Computing, Creative, Design & Innovation, Activity Book (Workbook), Cycle 01, Grade 2*, vol. 1. 2023-2024.

[97] Ministry of Education - UAE, *Computing, Creative, Design & Innovation, Student Book (Course Book), Cycle 01, Grade 1*, vol. 2. 2023-2024.

[98] Ministry of Education - UAE, *Computing, Creative, Design & Innovation, Student Book (Course Book), Cycle 01, Grade 2*, vol. 2. 2023-2024.

[99] Ministry of Education - UAE, *Computing, Creative, Design & Innovation, Student Book (Course Book), Cycle 01, Grade 3*, vol. 2. 2023-2024.

[100] Ministry of Education - UAE, *Computing, Creative, Design & Innovation, Student Book (Course Book), Cycle 01, Grade 4*, vol. 2. 2023-2024.

[101] Ministry of Education - UAE, *Computing, Creative, Design & Innovation, Student Book (Course Book), Cycle 02, Grade 5*, vol. 1. 2023-2024.

[102] Ministry of Education - UAE, *Computing, Creative, Design & Innovation, Activity Book (Workbook), Cycle 02, Grade 5*, vol. 1. 2023-2024.

[103] Ministry of Education - UAE, *Computing, Creative, Design & Innovation, Student Book (Course Book), Cycle 02, Grade 6*, vol. 1. 2023-2024.

[104] Ministry of Education - UAE, *Computing, Creative, Design & Innovation, Activity Book (Workbook), Cycle 02, Grade 6*, vol. 1. 2023-2024.

[105] Ministry of Education - UAE, *Computing, Creative, Design & Innovation, Student Book (Course Book), Cycle 02, Grade 7*, vol. 1. 2023-2024.

[106] Ministry of Education - UAE, *Computing, Creative, Design & Innovation, Activity Book (Workbook), Cycle 02, Grade 7*, vol. 1. 2023-2024.

[107] Ministry of Education - UAE, *Computing, Creative, Design & Innovation, Student Book (Course Book), Cycle 02, Grade 8*, vol. 1. 2023-2024.

[108] Ministry of Education - UAE, *Computing, Creative, Design & Innovation, Activity Book (Workbook), Cycle 02, Grade 8*, vol. 1. 2023-2024.

[109] Ministry of Education - UAE, *Computing, Creative, Design & Innovation, Student Book (Course Book), Cycle 02, Grade 5*, vol. 1. 2023-2024.

[110] Ministry of Education - UAE, *Computing, Creative, Design & Innovation, Activity Book (Workbook), Cycle 02, Grade 5*, vol. 2. 2023-2024.

[111] Ministry of Education - UAE, *Computing, Creative, Design & Innovation, Student Book (Course Book), Cycle 02, Grade 6*, vol. 2. 2023-2024.

[112] Ministry of Education - UAE, *Computing, Creative, Design & Innovation, Activity Book (Workbook), Cycle 02, Grade 6*, vol. 2. 2023-2024.

[113] Ministry of Education - UAE, *Computing, Creative, Design & Innovation, Student Book (Course Book), Cycle 02, Grade 7*, vol. 2. 2023-2024.

[114] Ministry of Education - UAE, *Computing, Creative, Design & Innovation, Activity Book (Workbook), Cycle 02, Grade 7*, vol. 2. 2023-2024.

[115] Ministry of Education - UAE, *Computing, Creative, Design & Innovation, Student Book (Course Book), Cycle 02, Grade 8*, vol. 2. 2023-2024.

[116] Ministry of Education - UAE, *Computing, Creative, Design & Innovation, Activity Book (Workbook), Cycle 02, Grade 8*, vol. 2. 2023-2024.

[117] Ministry of Education - UAE, *Computing, Creative, Design & Innovation, Student Book (Course Book), Cycle 03, Grade 9 General*, vol. 2. 2023-2024.

[118] Ministry of Education - UAE, *Computing, Creative, Design & Innovation, Activity Book (Workbook), Cycle 03, Grade 9 General*, vol. 2. 2023-2024.

[119] Ministry of Education - UAE, *Computing, Creative, Design & Innovation, Student Book (Course Book), Cycle 03, Grade 10 General*, vol. 2. 2023-2024.

[120] Ministry of Education - UAE, *Computing, Creative, Design & Innovation, Activity Book (Workbook), Cycle 03, Grade 10 General*, vol. 2. 2023-2024.

[121] Ministry of Education - UAE, 'Electives Model'. Accessed: Feb. 24, 2024. [Online]. Available: https://www.moe.gov.ae/En/MediaCenter/Announcements/Electives/Pages/default.aspx

[122] Ministry of Education - UAE, *Computing, Creative, Design & Innovation, Student Book (Course Book), Cycle 03, Grade 11 General*, vol. 2. 2023-2024.

[123] Ministry of Education - UAE, *Computing, Creative, Design & Innovation, Activity Book (Workbook), Cycle 03, Grade 11 General*, vol. 2. 2023-2024.

[124] Ministry of Education - UAE, *Computing, Creative, Design & Innovation, Student Book (Course Book), Cycle 03, Grade 12 General*, vol. 2. 2023-2024.

[125] Ministry of Education - UAE, *Computing, Creative, Design & Innovation, Activity Book (Workbook), Cycle 03, Grade 11 General*, vol. 2. 2023-2024.

[126] Ministry of Education - UAE, *Computing, Creative, Design & Innovation, Student Book (Course Book), Cycle 03, Grade 11 Advanced*, vol. 2. 2023-2024.

[127] Ministry of Education - UAE, *Computing, Creative, Design & Innovation, Activity Book (Workbook), Cycle 03, Grade 11 Advanced*, vol. 2. 2023-2024.

[128] Ministry of Education - UAE, *Computing, Creative, Design & Innovation, Student Book (Course Book), Cycle 03, Grade 12 Advanced*, vol. 2. 2023-2024.

[129] Ministry of Education - UAE, *Computing, Creative, Design & Innovation, Activity Book (Workbook), Cycle 03, Grade 12 Advanced*, vol. 2. 2023-2024.

[130] Commission for Academic Accreditation (CAA), 'Higher Education Institutions'. Accessed: Feb. 25, 2024. [Online]. Available: https://www.caa.ae/Pages/Institutes/All.aspx

[131] Commission for Academic Accreditation (CAA), ‘ Accredited Programs’. Accessed: Feb. 26, 2024. [Online]. Available: https://www.caa.ae/Pages/Programs/All.aspx

[132] Abu Dhabi Polytechnic, ‘Information Security Engineering Technology’. Accessed: Feb. 25, 2024. [Online]. Available: https://www.adpoly.ac.ae/information-security-engineering-technology/

[133] Abu Dhabi University, ‘Program Finder’. Accessed: Feb. 26, 2024. [Online]. Available: https://www.adu.ac.ae/study/programs/program-finder

[134] Ajman University, ‘Bachelor of Science in Information Technology’, Accessed: Feb. 26, 2024. [Online]. Available: https://www.ajman.ac.ae/en/academics/academic-programs-majors/programs/bachelor-of-science-in-information-technology

[135] Al Ain University, ‘Bachelor of Science in Cybersecurity’, Accessed: Feb. 26, 2024. [Online]. Available: https://engineering.aau.ac.ae/en/programs/bachelor-of-science-in-cybersecurity

[136] American University in the Emirates, ‘Bachelor of Science in Computer Science’, Accessed: Feb. 26, 2024. [Online]. Available: https://aue.ae/computer-science/

[137] American University in the Emirates, ‘Master in Security Studies and Information Analysis’, Accessed: Feb. 26, 2024. [Online]. Available: https://aue.ae/master-of-security-studies-and-information-analysis/

[138] Amity University Dubai, ‘BS Computer Science’. Accessed: Feb. 26, 2024. [Online]. Available: https://amityuniversity.ae/degree/bachelors-degree/engineering-architecture-and-interior-design/bachelor-of-technology-computer-science-engineering#degree-summary

[139] British University in Dubai, ‘Bachelor of Science in Computer Science – Cybersecurity’. Accessed: Feb. 26, 2024. [Online]. Available: https://www.buid.ac.ae/programmes/bachelor-of-science-in-computer-science-cybersecurity/

[140] British University in Dubai, ‘Master of Science (MSc) in Cybersecurity’. Accessed: Feb. 26, 2024. [Online]. Available: https://www.buid.ac.ae/programmes/mscincybersecurity/

[141] Canadian University Dubai, ‘Bachelor of Science in Cyber Security ’. Accessed: Feb. 26, 2024. [Online]. Available: https://www.cud.ac.ae/programs/undergraduate/engineering-applied-science-and-technology/bachelor-of-science-in-cyber-security

[142] Higher Colleges of Technology, ‘Bachelor of Information Technology’. Accessed: Feb. 26, 2024. [Online]. Available: https://hct.ac.ae/en/majors/bachelor-of-information-technology/

[143] Khalifa University, ‘BSc In Computer Science’. Accessed: Feb. 26, 2024. [Online]. Available: https://www.ku.ac.ae/program/bsc-in-computer-science

[144] Khalifa University, ‘MSc In Cyber Security’. Accessed: Feb. 26, 2024. [Online]. Available: https://www.ku.ac.ae/academics/graduate-programs/m-sc-in-cyber-security/

[145] Rochester Institute of Technology-Dubai, ‘Bachelor of Science in Computing Security’. Accessed: Feb. 26, 2024. [Online]. Available: https://www.rit.edu/dubai/programs/undergraduate/bachelor-science-computing-security

[146] Rochester Institute of Technology-Dubai, ‘Master of Science in Computing Security’. Accessed: Feb. 26, 2024. [Online]. Available: https://www.rit.edu/dubai/programs/graduate-programs/master-science-computing-security

[147] UAE University, ‘Bachelor of Science in Information Security’. Accessed: Feb. 26, 2024. [Online]. Available: https://www.uaeu.ac.ae/en/catalog/undergraduate/programs/bachelor-of-science-in-information-security.shtml

[148] UAE University, ‘Master of Science in Information Security’. Accessed: Feb. 26, 2024. [Online]. Available: https://www.uaeu.ac.ae/en/catalog/graduate/programs/master-of-science-in-information-security.shtml

[149] University of Dubai, ‘Master of Science in Cyber Security (MSCS)’. Accessed: Feb. 26, 2024. [Online]. Available: https://ud.ac.ae/ud_programs/master-of-science-in-cyber-security/

[150] University of Fujairah, ‘Bachelor of Information Technology’. Accessed: Feb. 26, 2024. [Online]. Available: https://uof.ac.ae/academics/cit/bit-networking-and-security/#1617619738979-593621c4-58fe

[151] University of Science and Technology of Fujairah, ‘Bachelor of Science in Information Technology Cyber Security’. Accessed: Feb. 26, 2024. [Online]. Available: https://ustf.ac.ae/index.php?p=engineering&s=bachelor-of-science-in-information-technology-cyber-security

[152] University of Sharjah, ‘Bachelor of Science in Cybersecurity Engineering’. Accessed: Feb. 26, 2024. [Online]. Available: https://www.sharjah.ac.ae/en/academics/Colleges/CI/dept/cep/Pages/Bachelor-of-Science-in-Cybersecurity-Engineering.aspx

[153] University of Sharjah, ‘Master of Science in Cybersecurity Engineering’. Accessed: Feb. 26, 2024. [Online]. Available:

https://www.sharjah.ac.ae/en/academics/Colleges/CI/dept/cep/Pages/Master-of-Science-in-Cybersecurity-Engineering.aspx#intro

[154] University of Wollongong in Dubai, 'Bachelor of Computer Science (Cyber Security)'. Accessed: Feb. 26, 2024. [Online]. Available: https://www.uowdubai.ac.ae/degrees/bachelors/computer-science/bachelor-computer-science-cyber-security#career-paths

[155] Zayed University, 'Bachelor of Science in Information Technology (Major in Security & Network Technologies)'. Accessed: Feb. 26, 2024. [Online]. Available: https://www.zu.ac.ae/main/en/colleges/colleges/__college_of_technological_innovation/index

[156] Zayed University, 'Master of Science in Information Technology (Cyber Security)'. Accessed: Feb. 26, 2024. [Online]. Available: https://www.zu.ac.ae/main/en/gsd/_graduate-degree-programs/master-of-science-in-information-technology

[157] International Organization for Standardization (ISO), 'ISO/IEC 27001:2022'. Accessed: Feb. 26, 2024. [Online]. Available: https://www.iso.org/standard/27001

[158] International Organization for Standardization (ISO), 'ISO/IEC 27002:2022'. Accessed: Feb. 26, 2024. [Online]. Available: https://www.iso.org/standard/75652.html

[159] National Institute of Standards and Technology (NIST), 'NIST Cybersecurity Framework'. Accessed: Feb. 26, 2024. [Online]. Available: https://www.nist.gov/cyberframework

[160] National Institute of Standards and Technology (NIST), ' NIST SP 800-50'. Accessed: Feb. 26, 2024. [Online]. Available: https://csrc.nist.gov/news/2023/nist-releases-draft-sp-800-50-rev-1

[161] Center for Internet Security (CIS), 'CIS Critical Security Controls'. Accessed: Feb. 26, 2024. [Online]. Available: https://www.cisecurity.org/controls

[162] International Organization for Standardization (ISO), 'ISO/IEC 27032:2023'. Accessed: Feb. 26, 2024. [Online]. Available: https://www.iso.org/standard/76070.html

[163] National Institute of Standards and Technology (NIST), 'NIST SP 800-53A'. Accessed: Feb. 26, 2024. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/53/a/r5/final

[164] P. Jerimy, 'Security Certification Roadmap'. Accessed: Feb. 29, 2024. [Online]. Available: https://pauljerimy.com/security-certification-roadmap/

[165] Tawzea, 'Tawzea'. Accessed: Apr. 19, 2024. [Online]. Available: https://www.tawzea.ae/

UAEU MASTER THESIS NO. 2024: 7

Cybersecurity threats and incidents continue to rise daily, presenting a widespread concern globally and in the UAE. This thesis underscores the crucial role of cybersecurity awareness in strengthening individual defenses and addresses the gaps and challenges in cybersecurity education. It presents a mobile application as a solution to help individuals in the UAE enhance their cybersecurity awareness and knowledge.

**Meera Alalawi** received her Master of Science in Information Security from the Department of Information Systems and Security, College of Information Technology at the United Arab Emirates University, UAE. She received her Bachelor of Information Technology, Security and Forensics from the Department of Computer and Information Science, Higher Colleges of Technology, Al Ain, UAE.