7-6-2024

TOWARDS A UNIFIED MODEL OF CYBERSECURITY LITERACY: BLENDING PEDAGOGICAL, PROFESSIONAL, CONCEPTUAL AND EMPIRICAL INSIGHTS

Andriani Piki
University of Central Lancashire Cyprus (UCLan Cyprus), Larnaca, Cyprus, apiki@uclan.ac.uk

Markos Markou
American University of Cyprus, Larnaca, Cyprus, markos.markou@aucy.ac.cy

Eliana Stavrou
Open University of Cyprus, Nicosia, Cyprus, eliana.stavrou@ouc.ac.cy

TOWARDS A UNIFIED MODEL OF CYBERSECURITY LITERACY: BLENDING PEDAGOGICAL, PROFESSIONAL, CONCEPTUAL AND EMPIRICAL INSIGHTS

Descriptive Case Study

Andriani Piki, University of Central Lancashire Cyprus (UCLan Cyprus), Larnaca, Cyprus, apiki@uclan.ac.uk

Markos Markou, American University of Cyprus, Larnaca, Cyprus, markos.markou@aucy.ac.cy

Eliana Stavrou, Open University of Cyprus, Nicosia, Cyprus, eliana.stavrou@ouc.ac.cy

Abstract

Recent technological advances illuminate the perplexing nature of cybersecurity which prevails as a rapidly expanding scientific field and a growing social concern, alike. Despite the wide diffusion of mobile technologies and wireless Internet connectivity, fundamental challenges and gaps still exist in terms of end-users' cybersecurity awareness, knowledge, skills, and behaviours. This study portrays a holistic understanding of cybersecurity literacy among non-experts, specifically in Wi-Fi contexts, by blending (i) innovative pedagogical approaches, (ii) professional cybersecurity frameworks, (iii) core cybersecurity knowledge areas and skills, and (iv) empirical insights gathered in the field from end-users, administrators of Wi-Fi networks, and cybersecurity experts. This four-tiered approach has informed the development of a unified model which can serve as a foundation for self-directed and personalised educational endeavours aiming to promote cybersecurity literacy among novice end-users.

Keywords: Cybersecurity Literacy, Cybersecurity Awareness, Skills Development, Empirical Study.

1 Introduction

The observation that individual users, social groups, and organisations rely heavily on the Web is not newfound. Online presence has become a vital necessity for individuals leveraging Web services and mobile applications for diverse educational, professional, entertainment, and social activities (Alsharif et al., 2022; Bragaru and Briceag, 2022; Saeed, 2023; Wetzig, 2022). Similarly, the Internet has long been established as a mission-critical constituent for organisations of all sizes and across industries, due to the unique features which designate the Web as a successful commercial medium (Laudon and Laudon, 2014). Alongside the benefits, excessive online presence poses numerous threats in terms of cybersecurity (Saeed, 2023), especially when connecting to insecure, public Wi-Fi networks. Therefore, it is crucial to ensure that end-users, owners/administrators of Wi-Fi networks, and other stakeholders are adequately educated on eminent cybersecurity threats so they can stay protected (Bragaru and Briceag, 2022; Saeed, 2023; Stavrou et al., 2024).

The initial motivation behind this study was the recurrent observation that individuals, across age groups and educational levels, spontaneously connect to free, open Wi-Fi hotspots available at public venues (including cafeterias, restaurants, shopping malls, museums, universities, airports, and hotel lobbies, amongst others), despite the impending cyberthreats associated with wireless networks. Therefore, exploring end-users', administrators', and experts' perceptions and experiences was presented as a timely and appealing opportunity. Another source of inspiration was the realisation that social and technological changes are often imposed on users, without thoroughly addressing training and educational needs or the implications of these changes on users' safety, privacy, and security. The

authors' expertise in diverse yet complementary areas of information systems (including cybersecurity, human-computer interaction, educational technology, and artificial intelligence), has stirred an inquiry around the professional frameworks and knowledge areas that currently inform curriculum development in cybersecurity education, as well as established pedagogical approaches and empirical insights which could further enrich the development of customised, self-directed educational endeavours for promoting cybersecurity literacy among non-experts. Drawing these four dimensions together, this study aims to craft a unified model that can guide curriculum development promoting cybersecurity literacy focusing specifically on the impending threats facing novice learners when connecting to public Wi-Fi networks. To realise this aim, the study starts with a discussion of related literature in Section 2, followed by an overview of pedagogical approaches employed in cybersecurity education and an exploration of prevalent cybersecurity frameworks, knowledge areas, and skills in Section 3. Section 4 describes the empirical case study conducted for gathering real-life insights from key stakeholder groups (experts, administrators/owners of Wi-Fi networks, and end-users) to explore their perceptions and level of awareness with regards to public Wi-Fi networks. Section 5 synthesises the four dimensions into a unified framework. Finally, Section 6 concludes our work and highlights avenues for further research and development for promoting cybersecurity literacy.

2 Background and Related Work

2.1 The Evolving Field of Cybersecurity

Historically, the evolution of technology has been accompanied by even more advanced infringing mechanisms implemented by attackers aiming to gain unauthorised access to Internet-connected devices, violate users' privacy, or render inoperable the Internet services on which they depend (Kurose and Ross, 2013). Wi-Fi networks, specifically, are susceptible to an array of cyberattacks: eavesdropping, Man-in-the-Middle (MitM); rogue hotspots; malware distribution illegitimately giving access to the users' personal data and device functionalities to attackers; social engineering (Stavrou et al., 2024); phishing (Cuchta et al., 2019; Wetzig, 2022); ransomware; cyber espionage (Scherb et al., 2023); cyberbullying (Procopiou et al., 2023); and data breaches (Bragaru and Briceag, 2022) among other threats (ENISA, 2020). Such threats can have significant legal, ethical, social, and financial implications for all stakeholders.

Recently, these phenomena have been intensified due to the changing jobs landscape and the rapid changes which accelerated the diffusion of technological innovations (IEEE Digital Reality, 2020). Undeniably, both technological transformations and security threats (Wetzig, 2022) have been accelerated due to the immense changes the world has experienced amidst Covid-19 pandemic. Mobile devices played a critical role during these challenging times enabling individuals to stay connected (Piki, 2020). Although social media apps were widely used before the pandemic, their context of use, and the extent to which users rely on these, have changed swiftly and immensely (Piki, 2020). Meanwhile, the educational, entertainment, and commercial capabilities of emerging technologies, such as Generative Artificial Intelligence (GenAI), Virtual Reality (VR), Internet of Things (IoT) devices, and Metaverse applications are relentlessly expanding. Their rapid diffusion is expected to magnify the impact of cyberthreats, leading to severe social and psychological effects on individual users (Procopiou et al., 2023) and adverse business and financial consequences for organisations (Piki et al., 2023). Hence, in addition to governmental and policy-making initiatives, raising awareness among non-experts (both end-users and administrators of Wi-Fi networks) is crucial.

2.2 The 'Digital Literacy Paradox'

The changing uses of Web-enabled technologies present an intriguing contradiction – the '*digital literacy paradox'*. On one hand, the number of users who proficiently use state-of-the-art digital technologies and mobile applications to communicate, socialise, collaborate, learn, and work, is increasing. Key enablers for this trend include the popularity of mobile applications (e.g., mobile

banking, learning, gaming, entertainment, m-commerce, and social media apps) (Bragaru and Briceag, 2022); the availability and flexibility of mobile devices; and the provision of affordable, high-speed wireless connections. Furthermore, in many cases organisational processes have been adapted, allowing the workforce to remain connected and work from anywhere, at any time, and 'on the go'.

On the other hand, to remain uninterruptedly connected, users may ignorantly connect to public Wi-Fi networks. These networks, however, are notoriously insecure and carry manifold risks. Recent data reveal that up to 22 billion user records were exposed in a single year (Singapore, 2022), a 300% increase in attacks was observed right after the outbreak of Covid-19 (Wetzig, 2022), approximately 80% of cybersecurity intrusions involve a human factor (Moumouh et al., 2023), while as many as 90% of data breaches occur as a result of phishing attacks, the attackers' favourite tactic to infiltrate a company's systems by tricking people into revealing sensitive information such as passwords or bank account details (Wetzig, 2022). These findings highlight that human error and lack of awareness constitute major threats to cybersecurity (Alsharif et al., 2022; Bragaru and Briceag, 2022; Piki et al., 2023; Saeed, 2023; Wetzig, 2022). Ultimately, they demonstrate that the extent of end-users' familiarity with using mobile apps and connecting to free Wi-Fi networks, is not analogous to their level of awareness of the underlying cybersecurity threats.

2.3 The Need for Upskilling and Reskilling

Ongoing technological advances have made cybersecurity knowledge and skills indispensable for every user, not just for computing professionals. Hence, there is a genuine necessity to identify the skillsets and knowledge areas which must be promoted in cybersecurity awareness-raising, training, and educational endeavours towards addressing the needs of diverse stakeholders. This is demonstrated by the IT Security Learning Continuum (Figure 1) proposed by NIST (Wilson and Hash, 2003).

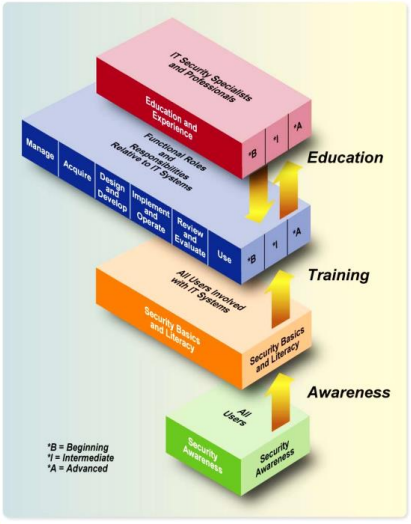

Figure 1. IT Security Learning Continuum (Wilson and Hash, 2003).

Evidently, cybersecurity awareness training and education are the most potent tools for defending users against cyberattacks. Identifying the factors leading to cyberattacks due to lack of awareness and human error (Figure 2) lies in the heart of such endeavours (Alsharif et al., 2022; Bragaru and Briceag, 2022; Piki et al., 2023; Saeed, 2023; Stavrou, 2023; Wetzig, 2022). Eliminating these factors could help prevent 19 out of 20 cyber breaches from taking place (Bragaru and Briceag, 2022).

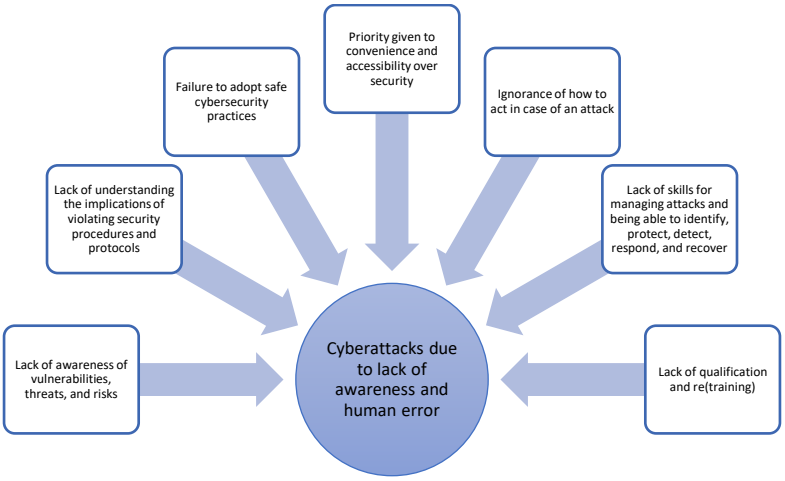

Figure 2. Human factors leading to cyberattacks.

There is a growing emphasis on upskilling and reskilling initiatives in the post-pandemic era (WEF, 2023), including the 'reskilling revolution' interactive tools (WEF, 2024a), and the promotion of the 'European Year of Skills' which aims to promote the visibility of continuous education and foster "*a fresh impetus for lifelong learning*" (EC, 2022) by launching forward-looking training endeavours and helping people gain in-demand skills. Such initiatives empower people to identity and develop the right skillsets and support companies in addressing skill and talent shortages in Europe (EC, 2022) and globally (WEF, 2024b). There are also cybersecurity-awareness programs and platforms by Microsoft, Cisco, Infosequre (2023), SANS (2024), QuickStart (2024), and other providers, offering a variety of customisable security training and cybersecurity awareness solutions that can be adjusted to fit the requirements of any individual and company, ranging from short courses, summer schools, and training camps, to courses leading to professional certifications in the field of cybersecurity (ISC^2, 2024; Kam et al., 2020). Addressing upskilling and reskilling needs requires taking a 'unified' view of cybersecurity literacy, one that is informed by pedagogical approaches, cybersecurity skills frameworks, cybersecurity knowledge areas, and empirical insights. This four-tiered approach is elaborated below.

3 Pedagogical, Professional, and Conceptual Insights

Educational endeavours can draw on various sources of knowledge depending on the learners' background, educational needs, and the context of learning (e.g., lifelong learning, upskilling/reskilling of company employees, end-users' awareness raising activities, etc.). In this study we blend four elements (i.e., pedagogical approaches, professional frameworks, cybersecurity concepts, and empirical insights) to form the basis for developing customised curricula addressing cybersecurity literacy for non-experts.

3.1 Innovative Pedagogies in Cybersecurity Education

Among the pedagogical approaches, which have been proposed in the broader context of cybersecurity education, the most relevant for promoting cybersecurity literacy among non-experts are those drawing on social constructivist and experiential learning theories. Indicative examples include embracing Digital Games-Based Learning (DGBL) for educating the workforce on prominent cyberthreats (Piki et al., 2023); utilising the Metaverse as an educational platform for educating minors on key security, safety, and privacy risks (Procopiou et al., 2023); and employing GenAI approaches for constructing a personalised cybersecurity learning plan (Kallonas et al., 2024). The latter is expected to attract a lot of attention in the coming years as learners are expected to increasingly utilise GenAI tools to prepare personalised study plans.

Purely for illustration purposes, a simple prompt such as "*Tell me what are the key cybersecurity skills that everyone needs to have*" on ChatGPT 3.5 (OpenAI, 2024) swiftly generated a comprehensive list of technical capabilities and soft skills (including 'ability to use cybersecurity tools such as intrusion detection systems', 'proficiency in developing risk mitigation strategies and implementing security controls', 'understanding the legal and ethical considerations', 'strong written and verbal communication skills' and 'capability to work collaboratively', amongst others). Remarkably, the generated response to this simple prompt acknowledged the importance of joining professional cybersecurity organisations, such as ISC^2 and ISACA, and prompted us to familiarise with key frameworks like NIST Cybersecurity Framework, ISO 27001, and GDPR. While the interplay between cybersecurity and AI is not new (Ansari et al., 2022; ENISA, 2023), the capabilities of GenAI tools for upskilling in cybersecurity is still underexplored (Kallonas et al., 2024). The open nature of such tools also makes them relevant for self-directed learning.

Several theoretical frameworks proposed with the view to inform and enrich cybersecurity education are also relevant when developing curricula and self-directed learning resources for non-experts, including the 'Cybersecurity Awareness Framework for Academia' (Khader et al., 2021); a theoretical framework for guiding the development of educational cybersecurity games (Hwang and Helser, 2022); a model developed to facilitate the creation of serious games for raising cybersecurity awareness among novice users (Le Compte et al., 2015); a framework for game design for mitigating phishing attacks (Arachchilage and Love, 2013); and a personalised cybersecurity training exercise based on learning theory (Chowdhury and Gkioulos, 2023). These efforts can promote self-directed and personalised learning contributing to developing non-experts' knowledge, skills, and cyber-resilience.

3.2 Professional Cybersecurity Frameworks

In addition to the innovative pedagogies discussed in the literature, a unified view of cybersecurity literacy can be enhanced by considering professional cybersecurity frameworks, some of which are highly relevant for raising cybersecurity literacy among non-experts. Embracing these skills-oriented frameworks (Figure 3) and tailoring them according to end-users' characteristics, learning needs, and educational objectives, can guide the development of enriched, personalised, and contextualised learning content, educational tools, and targeted assessments. Professional cybersecurity skills frameworks can also provide the foundation for extracting the essential knowledge areas to focus on when designing educational initiatives for promoting cybersecurity literacy.

Framework	Publishing Body	Overview: Scope & Purpose
Cybersecurity Framework	US National Institute of Standards and Technology (NIST, 2024)	Focuses on 5 functional areas to manage threats, namely: Identify, Protect, Detect, Respond, and Recover; serves as a foundation for addressing safety, privacy, and security risks.
European Cybersecurity Education and Professional Training	European Cyber Security Organisation (ECSO, 2022)	Specifies a baseline curriculum alongside best practices to cultivate fundamental cybersecurity competencies.
National Initiative for Cybersecurity Education (NICE)	US National Institute of Standards and Technology (NIST, 2020)	Serves as a reference source for developing content or tools that meet individual needs; provides guidance on different aspects of cybersecurity education, training, and workforce development.
General Data Protection Regulation (GDPR)	European Union (2016)	Protect the fundamental rights and freedoms of natural persons, particularly the right to the protection of their personal data.
Cyber Career Framework	UK cybersecurity council (2024)	Describes 16 cybersecurity specialisms, associated roles and responsibilities, and the required skills and knowledge
ISO/IEC 27001	International Standards Organisation (ISO, 2022)	Provides guidelines for establishing, implementing, maintaining, and continually improving an Information Security Management Systems (ISMS).
European Cybersecurity Skills Framework (ECSF)	European Union Agency for Cybersecurity (ENISA, 2018)	Recognises key professional cybersecurity roles and associated tasks, competencies, skills, and knowledge areas.
Code of Professional Ethics	Information Systems Audit and Control Association (ISACA, 2024)	Guides the professional and personal conduct of ISACA members.

Figure 3. Professional Cybersecurity Frameworks

3.3 Cybersecurity Knowledge Areas and Skills

Although the nature of educational initiatives promoting cybersecurity literacy will differ based on learners' skill needs and contextual factors, learning objectives can be broadly categorised under knowledge areas and skillsets related to cybersecurity principles and management, cybersecurity tools and techniques, and cybersecurity in modern and emerging digital technologies (ECSO, 2022). Educational initiatives need to be oriented around helping end-users gain an understanding of the properties of secure networks captured by the 'CIA triad' (confidentiality, integrity, and availability) (Kurose and Ross, 2013) and additional security objectives (authenticity of information, non-repudiation, and reliability) (Bragaru and Briceag, 2022); familiarise with security risks and types of attacks associated with public Wi-Fi networks (Figure 2); and develop the necessary skills and know-how to be able to utilise tools and protective measures for staying cyber-safe. These knowledge areas and skills can form the basis of cybersecurity literacy initiatives and can be further enhanced with empirical insights.

4 Case Study

4.1 Research Methodology and Study Participants

A case study was conducted to empirically explore cybersecurity awareness in the context of Wi-Fi hotspots offered by businesses in Cyprus as a complementary service to their customers. Primary data was gathered through 26 semi-structured interviews conducted with 2 cybersecurity experts (one female, one male), 9 network administrators/business owners (one of which is a computing expert), and 15 users of the free public Wi-Fi hotspots which were randomly selected (male and female, of different age groups and educational levels). Statistical analysis is beyond the scope of this study; rather, the aim of conducting interviews with these three groups of informants is to explore their perceptions and get deeper insights on their level of cybersecurity awareness. The interview responses were qualitatively analysed to identify recurrent or prominent patterns (Miles and Huberman, 1994). Verbatim quotes are used to portray a more meaningful and richer account of the informants' perceptions and experiences (Hammersley and Atkinson, 2019) and substantiate the researchers' interpretations.

4.2 Data Analysis and Key Findings

4.2.1 Insights from cybersecurity experts

The experts interviewed affirmed there is an evident lack of awareness both among users and Wi-Fi administrators/owners. They discussed users' tendency to consider password-protected Wi-Fi connections as secure which is certainly not the case since this password is shared. Open, public, free Wi-Fi networks "*are as safe as your browsing habits are. They are generally unsafe because everyone has access to them [...]. Even if they have a password, if someone has access to them and you are in the same network, they can sniff your traffic, get packets and analyse them, and use them maliciously […]. It depends on what you are doing, because if you are visiting an https site that has SSL certificate and the traffic is encrypted you are sort of OK. If you are visiting an http site then everything is open and anyone on the same network can view that, intercept that, and manipulate that.*" (Anna, Cybersecurity expert). Furthermore, when connecting to *"public Wi-Fi networks [....], even if they have a password, you're sharing a network with tons of other people, which means your data is at risk. Just because most wireless routers have a firewall to protect you from the Internet it doesn't mean you're protected from others connected to the same network. It's remarkably easy to steal someone's username and password or see what they're doing just by being on the same network. Therefore, open public Wi-Fi is not safe at all."* (Chris, Cybersecurity expert).

A noteworthy trend identified by both experts is that, increasingly, employers in Cyprus try to reduce the level of ignorance by training and educating their workforce. "*People in specific areas such as banks, auditing firms, telecommunication companies and the government have started becoming educated*

around cyberattacks and how to stay protected" (Chris). Business-wise, "*companies are paying attention [not only] because they have regulatory requirements, they have legal requirements, they have all those ISOs with which they need to comply, but also because if the company does not carefully consider security issues and they get hacked, then it's all over the Internet, they cannot hide it, and it will negatively impact their reputation*" (Anna). Nevertheless, even though some users may be cautious of security issues in their workplace networks, they do not seem to take into consideration the underlying risks when connecting to public networks. "*The younger generation is more aware of cybersecurity nowadays. But again, due to our nature most of the time we do not take into consideration the risks when connecting to vulnerable networks such as public, open Wi-Fi hotspots*" (Chris). This illustrates how the urge for online presence often overrides the need for securing our devices and personal data.

According to the experts interviewed, a high degree of ignorance is also attributed to administrators of Wi-Fi hotspots. Very few public Wi-Fi hotspots (only one in our study, whose administrator has a computing background) provide a safe networking environment. Businesses such as cafeterias, restaurants, or hair salons are not typically concerned with securing their networks due to three main reasons: lack of awareness of the frequency and ease with which wireless networks can be compromised; lack of technical skills and knowledge regarding maintenance and proper administration of hardware and software needed to secure the network; and finally, cost. This observation is corroborated by the findings discussed in the literature (Osborn and Simpson, 2017; Stavrou et al., 2024). Most administrators simply obtain their Internet Service Provider (ISP)'s router and plug it in without re-configuring it or changing the default password. As a result, their network is at risk since "*those routers have very specific algorithms of computing the key you must enter to access the Wi-Fi. There is an application that cracks that, and you can download it on your phone, and you can just walk around and connect to Wi-Fi. Admins don't change the password, don't change the SSID, because they just don't know*" (Anna). Another commonly observed habit is that they ignorantly restart the affected devices/routers when unknown issues occur, failing both to investigate the potential causes and to take measures towards protecting their network and their clients from cyberattacks. This further illustrates the lack of awareness, knowledge, skills, and competences.

Coupled with the lack of awareness, cost was also a recurring justification. It is "*a considerable investment as most of the solutions are based on user licenses and concurrent sessions. That is why for small business, like cafeterias and restaurants such investment may be prohibitive […] in terms of initial cost and on-going maintenance. To build a secure environment needs proper administration and daily maintenance that increase the overall cost*" (Chris). This is a classic case of owners not allocating budget in actions that will not result in direct monetary returns (Osborn and Simpson 2017), including training (Stavrou et al., 2024), since Wi-Fi is generally provided as a free service to customers.

When asked about the ease, frequency, and severity of hacking attacks today, the experts verified that attackers may harm unsuspected users connected to public, free Wi-Fi networks, in a variety of ways, and at a remarkable ease. *"It's really easy to make an attack today. You have what we call script kiddies, [who] can find online scripts and programs like Kali Linux [and] use them to attack someone. There is also organised crime."* (Anna). Attackers can gain access to usernames and passwords (e.g., e-banking, email, online utility bills, etc.) through pharming, phishing, or packet sniffing. They can also redirect traffic through DNS poisoning, and generally monitor users' actions or compromise users' devices through a MitM attack. The latter is used as a mediating phase for launching other attacks. *"If someone has access to the router, they can manipulate the DNS records, so if you visit Facebook, I can manipulate that and make you visit [...] a malicious website. Then, I can use the website for a phishing attack using a log-in prompt. Users enter a username and password, and I can use these to infect their computer by loading a virus for example"* (Anna).

Additionally, the specialists provided recommendations and countermeasures for administrators and users of public Wi-Fi networks to safeguard their networks and devices from attacks. For administrators, the experts recommended using Intrusion Detection System (IDS) and Intrusion Prevention Systems (IPS), providing VPN connection over open Wi-Fi, using advanced firewall, URL filtering, threat emulation, and wireless client isolation, amongst others. For users, suggestions ranged from trivial measures, such as turning Wi-Fi off when not needed, to more meticulous ones, such as using an updated

antivirus software and having firewall enabled, being vigilant of phishing attacks, using VPN connections, preferably using their ISP's mobile network, visiting only secure HTTPS sites and checking the site's certificate. Essentially, "*the effort should also be concentrated on educating people to take necessary precautions when using public open Wi-Fi, at least when they are performing specific operations [such as] Internet banking transactions and connecting to corporate resources"* (Chris). This is aligned with relevant literature suggesting that one of the most important countermeasures against cybersecurity attacks entails educating users, increasing user awareness, and involving users in identifying common types of attacks (Alsharif et al., 2022; Bragaru and Briceag, 2022; Chowdhury and Gkioulos, 2023; Piki et al., 2023; Saeed, 2023; Stavrou et al., 2024).

4.2.2 Insights from administrators of free public Wi-Fi networks

For triangulation purposes, in addition to the in-depth insights gathered from experts, data was also collected from administrators of Wi-Fi hotspots to explore current practices in the context of small businesses in Cyprus. Seven out of nine administrators admitted they lack the necessary technical knowledge to setup and maintain a secure Wi-Fi network and rely on the default ISP settings. Furthermore, the administrators of the eight password-protected networks incorrectly assumed their networks are secure ignoring the fact that having passwords on display nullifies their usefulness and relegates the networks' protection to the same level as open Wi-Fi networks. Six administrators admitted they have never changed the password since they first installed their network while two administrators changed the password only once. When asked whether any of their customers ever experienced a security threat or attack while being connected to their network, all nine responded negatively. However, even if an attack did occur, it is unlikely that administrators or users would be in position to recognise the cause of the attack. These facts demonstrate the overall lack of cybersecurity awareness.

4.2.3 Insights from end-users

The analysis of end-users' responses also demonstrated an overall lack of awareness of the dangers associated with Wi-Fi networks and the means of protecting their devices from being compromised. 13 out of 15 users admitted that connecting to Wi-Fi networks is the first thing they do when such networks are available. The remaining users (who have an IT-related background) explained they are conscious of the dangers inherent in shared networks and generally prefer using their mobile data, yet may still connect depending on the urgency (in one case, urgency was defined as their children begging for YouTube videos!). These knowledgeable users explained that when they connect, they do so for a limited amount of time, only if the venue is not crowded, and they never access or provide sensitive/personal information. They also disconnect from the network as soon as they have performed the necessary tasks. The findings illuminate a multifaceted relationship among users' level of expertise regarding privacy concerns, their emotional responses, and their coping behaviours in the context of privacy and security threats (Jung and Park, 2018). Therefore, the importance of human factors should not be underestimated (Bragaru and Briceag, 2022; Cuchta et al., 2019; Wetzig, 2022).

Another interesting finding was the fact that despite attributing high value to their personal information (e.g., photographs, date of birth, usernames and passwords, etc.) all fifteen respondents would connect (under certain circumstances) to a public Wi-Fi network. The discrepancy between the value users assign to their privacy information and their actual behaviour is referred to as the 'privacy paradox phenomenon', suggesting that "users actively share personal information despite their concerns, because they do not only consider risk but also the expected benefit" (Kokolakis, 2017, p. 125). Individuals will connect to potentially insecure networks and may be willing to reveal personal information for relatively small rewards, often just for accessing social networks (Kokolakis, 2017). Overall, the insights provided by analysing the interview data from users, administrators, and security specialists re-emphasised what has been suggested in the studied literature.

5 Unified Model of Cybersecurity Literacy

The goal of this study is to blend pedagogical, professional, conceptual, and empirical insights with the view to enrich self-directed and lifelong learning efforts towards promoting cybersecurity literacy and addressing cybersecurity skills gaps among non-experts. Firstly, embracing technology-enhanced, learner-centred, personalised educational approaches provides the cornerstone for activating learner's interest and motivation to develop the knowledge, skills, attitudes, and behaviours required for becoming cyber-resilient. Secondly, drawing on skills-based frameworks provides a good ground for ensuring that fundamental skills, as well as ethical and social responsibilities, are embedded in educational activities. Thirdly, the fusion of learning objectives and security objectives is deemed necessary for extracting the learning content, knowledge areas, and skillsets to be covered during reskilling/upskilling journeys. Finally, integrating empirical insights into the formula affords a unique perspective on prevalent challenges and skills gaps in cybersecurity, strengthening the findings extracted from the literature, and enriching the proposed unified model of cybersecurity literacy (Figure 4).

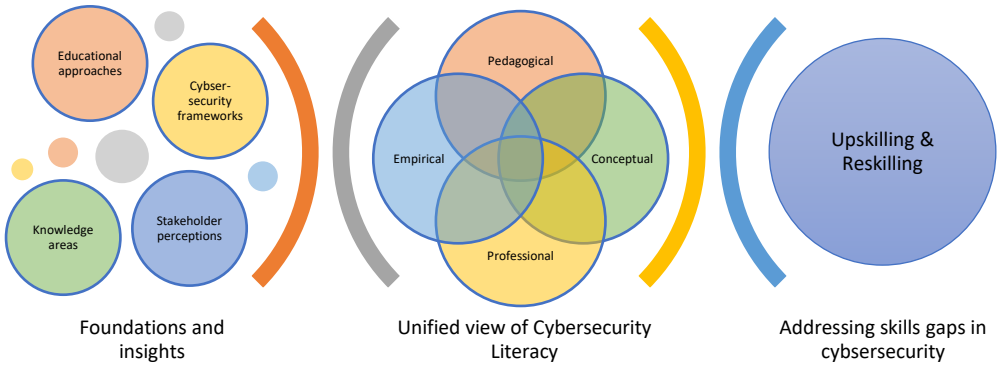

Figure 4. The proposed unified model of cybersecurity literacy.

6 Discussion and Conclusion

Cybersecurity constitutes an important field of study given the proliferation of Internet-connected devices and the diversity of end-users. Although one would assume that the widespread use of Web-based technologies by individuals, and the overreliance of many businesses on the services afforded by these technologies, would encourage a better understanding of how to protect against cyberthreats, the empirical and bibliographical insights we gathered have revealed that this is (still) not the case. As cyberattacks become increasingly more sophisticated, intelligently targeted, and harder to detect (ENISA, 2020), the need for (re)training end-users to identify, detect, and combat such threats is more relevant than ever before (Moumouh et al., 2023; Piki et al., 2023; Saeed, 2023; Scherb et al., 2023; Stavrou, 2020). This need entails considering cybersecurity not just as a priority for computing professionals, but also as an educational need for all end-users who connect to the Internet. This study contributes to ongoing awareness-raising endeavours by presenting a unified model of cybersecurity literacy, building on what we already know from established cybersecurity frameworks and core cybersecurity knowledge areas and skills, and enriching this knowledge with relevant innovative educational approaches and empirical insights gathered in the field. It is hoped that this model can advance contemporary educational efforts towards promoting cybersecurity literacy among all stakeholders.

Interviewing administrators/owners of free Wi-Fi networks revealed lack of awareness of the underlying security concerns, illiteracy in terms of fundamental cybersecurity concepts, and limited technical knowledge to properly setup and maintain a secure Wi-Fi network. The lack of awareness was also echoed in the insights gathered from end-users. Free, public networks present a convenient and cost-

efficient way to access online accounts, post on social media apps, catch up on work, and check emails while on the go. Most users appear oblivious of the fact that such networks are vulnerable to cyberattacks (Stouffer, 2022). While the prevalence of such insecure, free, public Wi-Fi networks increases the possibility of being hacked, posing threats to privacy, safety, and confidentiality, the users' desire to be constantly connected overrides cybersecurity objectives (Kokolakis, 2017). Therefore, given the complexity of cybersecurity, and the need to educate the public (end-users and Wi-Fi administrators/owners), a multifaceted approach to education is required, combining professional cybersecurity frameworks, knowledge areas and skills, with empirical insights and innovative pedagogical approaches.

Avenues for extending this work include designing new cybersecurity curricula for self-directed and personalised lifelong learning or validating existing educational games, tools, platforms, training courses and other resources based on the proposed unified model of cybersecurity literacy; conducting larger-scale case studies and action research to further explore the experiences, behaviours, attitudes, skills, and perceptions of diverse user groups and involve them in educational and curriculum development activities; as well as embracing novel technologies and pedagogical approaches in the design of forward-thinking cybersecurity educational programmes for raising cybersecurity literacy among non-experts, placing special emphasis on human factors.

References

Alsharif, M., Mishra, S., and AlShehri, M. (2022). "Impact of Human Vulnerabilities on Cybersecurity," *Computer Systems Science and Engineering*, 40(3).

Ansari, M. F., Dash, B., Sharma, P., and Yathiraju, N. (2022). "The impact and limitations of artificial intelligence in cybersecurity: a literature review," *International Journal of Advanced Research in Computer and Communication Engineering*.

Arachchilage, N. A. G., and Love, S. (2013). "A game design framework for avoiding phishing attacks," *Computers in Human Behavior*, 29(3), 706-714.

Bragaru, T., and Briceag, V. (2022). "Sustainable cybersecurity training for modern society," *ARA Journal of Sciences*, 30.

Chowdhury, N., and Gkioulos, V. (2023). "A personalized learning theory-based cyber-security training exercise," *International Journal of Information Security*, 22(6), 1531-1546.

Cuchta, T., Blackwood, B., Devine, T.R., Niichel, R.J., Daniels, K.M., Lutjens, C.H., Maibach, S. and Stephenson, R.J (2019). "Human risk factors in cybersecurity," *20th Annual SIG conference on Information Technology Education*, 87-92.

EC (2022). *European Year of Skills 2023*. European Commission, URL: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-year-skills-2023_en (accessed on January 19, 2024).

ENISA (2018). *European Cybersecurity Skills Framework (ECSF)*, ENISA, URL: https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework (accessed on February 12, 2024).

ENISA (2020). *ENISA Threat landscape 2020: Cyber attacks becoming more sophisticated, targeted, widespread and undetected*. URL: https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020 (accessed on February 23, 2024).

ENISA (2023). *Artificial Intelligence and cybersecurity research*, ENISA, URL: https://www.enisa.europa.eu/publications/artificial-intelligence-and-cybersecurity-research (accessed on February 27, 2024).

ESCO (2022). *European cybersecurity education and professional training: Minimum reference curriculum*. European Cyber Security Organisation (ECSO), URL: https://ecs-org.eu/ecso-uploads/2022/12/2022_SWG5.2_Minimum_Reference_Curriculum_final_v3.0.pdf (accessed on March 16, 2024).

EUR-Lex (2016). *General Data Protection Regulation*, Europa.eu, URL: https://eur-lex.europa.eu/eli/reg/2016/679/2016-05-04 (accessed on March 18, 2024).

Hammersley, M., and Atkinson, P. (2019). *Ethnography*: Principles in Practice. Routledge.

Hwang, M. I., and Helser, S. (2022). "Cybersecurity educational games: a theoretical framework." Information and Computer Security, 30(2), 225-242.

IEEE Digital Reality (2020). *Digital Transformation*. IEEE Digital Reality Initiative White Paper. URL: https://digitalreality.ieee.org/images/files/pdf/DRI_White_Paper_-_Digital_Transformation_-_Final_25March21.pdf (accessed on January 12, 2024).

Infosequre (2023). *Navigate the great risks and rewards of the digital world - Security awareness solutions*. URL: https://www.infosequre.com/ (accessed on March 15, 2024).

ISACA (2024). *Code of Professional Ethics*. Information Systems Audit and Control Association (ISACA), URL: https://www.isaca.org/code-of-professional-ethics (accessed on March 16, 2024).

ISC^2 (2024). *Cybersecurity workforce study 2023: Revealing New Opportunities for the Cybersecurity Workforce*, International Information System Security Certification Consortium (ISC^2), URL: https://www.isc2.org/research (accessed on March 14, 2024).

ISO (2022). ISP/IEC 27001:2022. *Information security, cybersecurity and privacy protection – Information Security Management Systems*, URL: https://www.iso.org/standard/27001 (accessed on March 16, 2024).

Jung, Y., and Park, J. (2018). "An investigation of relationships among privacy concerns, affective responses, and coping behaviors in location-based services," *International Journal of Information Management*, 43, 15-24.

Kallonas, C., Piki, A., Stavrou, E. (2024). "Empowering Professionals: A Generative AI Approach to Personalized Cybersecurity Learning," *IEEE Global Engineering Education Conference (EDUCON 2024)*, Kos, Greece.

Kam, H.-J., Menard, P., Ormond, D., and Crossler, R. E. (2020). "Cultivating cybersecurity learning: An integration of self-determination and flow," *Computers and Security*, 96(101875). doi:10.1016/j.cose.2020.101875.

Khader, M., Karam, M., and Fares, H. (2021). "Cybersecurity awareness framework for academia,". *Information*, 12(10), 417.

Kokolakis, S. (2017). "Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon," *Computers and Security*, 64, 122-134.

Kurose, J. F., and Ross, K. W. (2013). *Computer networks: a top-down approach*, 6th Edition. Pearson Education (International edition).

Laudon, K. C., and Laudon, J. P. (2014). *Management Information Systems: Managing the Digital Firm*. Pearson.

Le Compte, A., Elizondo, D., and Watson, T. (2015). "A renewed approach to serious games for cyber security," *7th International Conference on Cyber Conflict: Architectures in Cyberspace 2015*, 203-216, IEEE.

Miles, M. B., and Huberman, A. M. (1994). *Qualitative data analysis: An expanded sourcebook*. Sage.

Moumouh, C., Chkouri, M. Y., and Fernández-Alemán, J. L. (2023). "Cybersecurity awareness through serious games: A systematic literature review," *International Conference on Networking, Intelligent Systems and Security*, 190-199, Springer, Cham.

NIST (2020). *Workforce framework for cybersecurity, National Initiative for Cybersecurity Education (NICE)*, National Institute of Standards and Technology, URL: https://csrc.nist.gov/pubs/sp/800/181/r1/final (accessed on February 11, 2024).

NIST (2024). *Cybersecurity Framework*, National Institute of Standards and Technology, URL: https://www.nist.gov/itl/smallbusinesscyber/planning-guides/nist-cybersecurity=framework (accessed on February 11, 2024).

OpenAI (2024.). *ChatGPT*, URL: https://chat.openai.com/ (accessed on March 11, 2024).

Osborn, E., and Simpson, A. (2017). "On small-scale IT users' system architectures and cyber security: A UK case study," *Computers and Security*, 70, 27-50.

Piki, A. (2020). "An exploration of student experiences with social media and mobile technologies during emergency transition to remote education." *World Conference on Mobile and Contextual Learning* (mLearn 2020), 10-17.

Piki, A., Stavrou, E., Procopiou, A., and Demosthenous, A. (2023). "Fostering Cybersecurity Awareness and Skills Development Through Digital Game-Based Learning," *10th International Conference on Behavioural and Social Computing (BESC 2023)*, 1-9, IEEE.

Procopiou, A., Piki, A., Stavrou, E., and Zeniou, N. (2023). "Free guy or bad guy: Safety, privacy, and security risks for minors in the Metaverse and prominent educational considerations," *International Conference on Human-Computer Interaction (HCII 2023)*, pp. 445-460.

QuickStart (2024). *Transform Your IT Skills and Future-Proof Your Career with IT Training*. URL: https://www.quickstart.com/ (accessed on March 21, 2024).

Saeed, S. (2023). "Education, Online Presence and Cybersecurity Implications: A Study of Information Security Practices of Computing Students in Saudi Arabia," *Sustainability*, 15(12), 9426.

SANS (2024). *Cyber Security Training, Certifications, Degrees and Resources*, SANS, URL: https://www.sans.org/emea/ (accessed on March 21, 2024).

Scherb, C., Heitz, L. B., Grimberg, F., Grieder, H., and Maurer, M. (2023). "A serious game for simulating cyberattacks to teach cybersecurity," *arXiv preprint*, arXiv:2305.03062.

Singapore, C. (2022). *The top 10 cybersecurity games your employees need to play*. URL: https://potatopirates.game/blogs/cybersecurity/the-top-10-cybersecurity-games-your-employees-need-to-play (accessed on January 15, 2024).

Stavrou, E. (2020). "Back to basics: towards building societal resilience against a cyber pandemic," *Journal on Systemics, Cybernetics and Informatics*, 18(7), 73-80.

Stavrou, E. (2023). "Planning for Professional Development in Cybersecurity: A New Curriculum Design," *IFIP International Symposium on Human Aspects of Information Security and Assurance (HAISA)*.

Stavrou, E., Piki, A., and Varnava, P. (2024). "Merging Policy and Practice: Crafting Effective Social Engineering Awareness-Raising Policies," *10th International Conference on Information Systems Security and Privacy (ICISSP 2024)*.

Stouffer, C. (2022). *Public Wi-Fi: An ultimate guide on the risks + how to stay safe*, Norton.com, URL: https://us.norton.com/blog/privacy/public-wifi (accessed on November 12, 2023).

UK Cyber Security Council (2024). *Voice for the UK's cyber security profession*. UK Cyber Security Council, URL: https://www.ukcybersecuritycouncil.org.uk/ (accessed on February 17, 2024).

WEF (2023). *The future of Jobs Report 2023*. World Economic Forum. URL: https://www.weforum.org/publications/the-future-of-jobs-report-2023/ (accessed on January 15, 2024).

WEF (2024a). *Reskilling Revolution: Insights and Tools*. World Economic Forum, URL: https://initiatives.weforum.org/reskilling-revolution/insights-tools (accessed on January 19, 2024).

WEF (2024b). *World Economic Forum: The Global Risks Report 2024*, URL: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf (accessed on March 15, 2024).

Wetzig, C. (2022). *15 Alarming Cybersecurity Facts and Statistics*, ThriveDX, URL: https://thrivedx.com/resources/article/cyber-security-facts-statistics?referrer=cybint (accessed on March 2, 2024).