education sciences

MDPI

Article

MoonPhase: An Instructional Framework for Portable Experiential Cybersecurity Learning in Engineering Education

Ricardo Lopes da Silva [1], Luís Miguel Barata [1,2,3,*] and Ângela Cristina Marques de Oliveira [1,4,*]

[1] Department of Computer Science, Polytechnic University of Castelo Branco, 6000-084 Castelo Branco, Portugal; ricardosilva2@ipcbcampus.pt
[2] NOVA Laboratory for Computer Science and Informatics (NOVA LINCS), Department of Computer Science, University of Beira Interior, 6201-001 Covilhã, Portugal
[3] Instituto de Telecomunicações, Department of Computer Science, University of Beira Interior, 6201-001 Covilhã, Portugal
[4] Research Centre in Digital Services (CISeD), 3500-064 Viseu, Portugal
* Correspondence: luis.barata@ipcb.pt (L.M.B.); angelaoliveira@ipcb.pt (Â.C.M.d.O.)

Abstract

In an age of pervasive connectivity and rapidly evolving cyber threats, cybersecurity has become a transversal competency in engineering education rather than a niche specialism. This paper presents MoonPhase, a multifunctional portable device based on a Raspberry Pi platform, designed to support experiential cybersecurity learning in engineering education contexts by integrating offensive, defensive, and educational modes into a single physical artefact. The work builds on a structured literature review, with study identification and selection documented using a PRISMA 2020-informed flow diagram, and a state-of-the-art analysis of portable cybersecurity tools to derive design requirements that balance realism, safety, and pedagogical alignment. MoonPhase combines sub-GHz replay capabilities, 2.4 GHz interference and monitoring, fake Wi-Fi access points, packet sniffing, and network scanning in a compact, menu-driven platform that can be deployed in regular laboratories and outreach workshops. The paper describes the hardware and software architecture of the device and its instructional framing, linking device functionalities to learning outcomes, laboratory activities, ethical reflection, and assessment. A preliminary educational pilot was conducted with 21 undergraduate students using a 90 min session and a one-group pre-test/post-test design. Mean knowledge scores increased from 5.86 ± 1.42 to 8.24 ± 1.00, corresponding to an average gain of 2.38 points. A paired-samples t-test confirmed a statistically significant difference ($t(20) = 14.744$, $p < 0.001$), with a large within-participant effect size (Cohen's $d_z = 3.217$). Students also reported high levels of perceived authenticity (4.38/5), engagement (4.57/5), and self-reported ethical awareness (4.29/5). These exploratory results provide preliminary empirical support for the proposed instructional framework, while the small sample size and absence of a control group limit causal interpretation. MoonPhase is positioned as a replicable educational resource that brings students closer to realistic attack and defence scenarios in controlled settings.

Keywords: engineering education; cybersecurity; experiential learning; portable devices; wireless networks

Check for updates

Academic Editors: Eva Ordóñez-Olmedo, Pilar Gómez-Rey, Isotta Mac Fadden and Lourdes Belén Espejo Villar

Received: 30 May 2026
Revised: 2 November 2026
Accepted: 5 November 2026
Published: 10 November 2026

Copyright: © 2026 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license.

1. Introduction

Engineering education increasingly takes place in a world characterised by uncertainty, complexity and tightly coupled socio-technical systems. Cyber–physical infrastructures, ubiquitous wireless communication and pervasive Internet of Things (IoT) deployment

expose societies to novel forms of risk, including large-scale cyberattacks, data breaches and disruptions of essential services European Union Agency for Cybersecurity (2025); Europol (2024). In this context, cybersecurity is no longer an optional specialisation but a transversal competency that cuts across engineering disciplines, requiring graduates to reason about vulnerability, resilience and ethics in complex environments.

Recent reports from European and international agencies highlight the growth of attacks on public Wi-Fi networks, the widespread use of social engineering, and the impact of low digital literacy on the success of security incidents European Union Agency for Cybersecurity (2025); Pawlicka et al. (2023). This situation puts pressure on higher education institutions and training providers not only to update curricular content, but also to design learning experiences that help students deal with uncertainty, contested information and evolving threat landscapes.

Portable devices for security auditing and experimentation, such as Flipper Zero, Pwnagotchi or LilyGO boards, have shown the potential of compact platforms to simulate attacks, detect vulnerabilities and support gamified learning activities Evilsocket (2023); Flipper Devices Inc. (2023); LilyGO (2023). However, many of these solutions are not primarily designed for educational settings and rarely offer explicit pedagogical framing, alignment with programme-level learning outcomes or integrated assessment strategies Luh et al. (2025); Phuong et al. (2023). As a result, instructors who wish to use such tools often need to design bespoke activities and deal with tensions between demonstration value, safety and ethical considerations.

Despite the growing availability of cybersecurity tools and experiential learning environments, a practical gap remains in undergraduate engineering education. Existing solutions are often either technically oriented tools with limited pedagogical structure or resource-intensive environments that are difficult to deploy in regular laboratory settings. This creates a need for portable and replicable platforms that combine realistic cybersecurity experimentation with explicit learning outcomes, guided activities, ethical reflection, and assessment. MoonPhase was designed to address this gap by integrating offensive, defensive, and educational functionalities into a single physical artefact intended for supervised use in engineering education.

In parallel, research on cybersecurity education, workshops and serious games has emphasised the importance of experiential and system-level learning activities that allow students to observe and interact with realistic attack and defence scenarios T. Nguyen et al. (2024); Rege (2015). Studies report that hands-on workshops in IT/OT environments and gamified simulations of cyber–physical systems can increase engagement, improve risk comprehension and support adversarial risk exploration in a controlled manner Luh et al. (2025); Phuong et al. (2023). From the perspective of engineering education, these findings suggest that effective cybersecurity teaching requires more than transferring technical knowledge: learners must engage with authentic, uncertain situations, reason about human and organisational factors, and reflect on their own responsibilities when operating powerful tools.

MoonPhase was conceived as a multifunctional portable cybersecurity device that responds to these challenges. It balances offensive, defensive and educational functionalities in a modular architecture based on a Raspberry Pi Zero 2 W and dedicated wireless communication modules, but it is also explicitly framed as an educational artefact for engineering programmes.

The device design is grounded in a structured literature review combining database searches and supplementary identification of relevant studies, with the selection process documented using a PRISMA 2020-informed flow diagram. The main goal was to identify gaps in existing tools regarding explicit educational framing and integration into curric-

ula Luh et al. (2025); Page et al. (2021); Phuong et al. (2023). MoonPhase was developed across two project-based courses (Project I and Project II) in an undergraduate programme, following an iterative cycle from the literature review and requirements elicitation to prototyping, integration and reflection Silva (2026a, 2026b). This trajectory reflects how authentic design projects can cultivate students' ability to navigate uncertainty and complexity in engineering practice.

Accordingly, the present manuscript is framed as a design and instructional framework study for MoonPhase, complemented by a preliminary empirical evaluation of its educational use. In addition to describing the development and curricular integration of the platform, the study reports the results of an exploratory pilot conducted with 21 undergraduate students using a 90 min MoonPhase-based learning session.

The contributions of this paper are threefold:

- to present the design and implementation of MoonPhase as a portable cybersecurity artefact explicitly conceived for engineering education contexts;
- to articulate an instructional framework that links the device's offensive, defensive, and educational modes to learning outcomes, classroom activities, assessment, and ethical reflection;
- to provide a preliminary empirical evaluation of the proposed framework through an exploratory pilot study involving 21 undergraduate students, examining knowledge gains, perceived authenticity, engagement, and ethical awareness.

The study therefore combines the design and implementation of MoonPhase with a pedagogically grounded instructional framework and an exploratory educational evaluation. The pilot study provides preliminary quantitative evidence regarding changes in students' cybersecurity knowledge and their perceptions of authenticity, engagement, and ethical responsibility. Given the limited sample size and the absence of a control group, the empirical component is intended as an initial evaluation rather than a definitive assessment of educational effectiveness.

The proposed design aligns with calls in the cybersecurity education literature for experiential, system-level learning activities that expose students to realistic scenarios while maintaining safety and ethical oversight Narain et al. (2025); Rege (2015). In this sense, MoonPhase is intended not only as a technical artefact, but as a contribution to the broader discussion on how engineering education can respond to uncertainty and complexity in digital societies.

2. Related Work

2.1. Systematic Review on Portable Cybersecurity Devices

During the first phase of the project, a structured literature review was conducted to identify research on portable cybersecurity devices, security auditing tools, and educational approaches to cybersecurity. The review employed a documented search and selection process, complemented by targeted identification of relevant studies through additional sources. The identification and selection stages are reported using a PRISMA 2020-informed flow diagram Page et al. (2021). The purpose of the review was not only to catalogue existing cybersecurity tools, but also to identify design characteristics relevant to educational use. In particular, the analysis examined portability, technical scope, offensive and defensive capabilities, educational integration, support for experiential activities, and the extent to which ethical or reflective components were explicitly incorporated.

The primary database search was conducted on 25 October 2025 using ScienceDirect and the ACM Digital Library. ScienceDirect was used to retrieve research articles, whereas the ACM Digital Library search was restricted to books and book-related publications after

an initial broader search returned a large number of results. The search strategy combined terms related to penetration testing, ethical hacking, security auditing, portable computing platforms, wireless technologies, and educational applications. Two additional studies were identified through supplementary Google searches and retrieved from arXiv. The search expression and the procedures used for identifying and selecting studies are documented in Appendix C.

The eligibility criteria considered studies published between 2020 and 2025, written in English or Portuguese, and relevant to the research questions concerning portable cybersecurity technologies, offensive and defensive security, and educational applications. Studies outside the publication period, unrelated to cybersecurity, or without a relevant connection to the review questions were excluded. The database searches identified 132 records, comprising 124 from ScienceDirect and 8 from the ACM Digital Library. Following title and abstract screening, 119 records were excluded, leaving 13 reports for full-text assessment. Two additional reports, identified through supplementary Google searches and retrieved from arXiv, were also considered. Consequently, 15 reports underwent full-text eligibility assessment, of which six were excluded and nine were retained for the final synthesis Silva (2026a). The study identification and selection process is illustrated in Figure 1, while additional methodological details are provided in Appendix C.

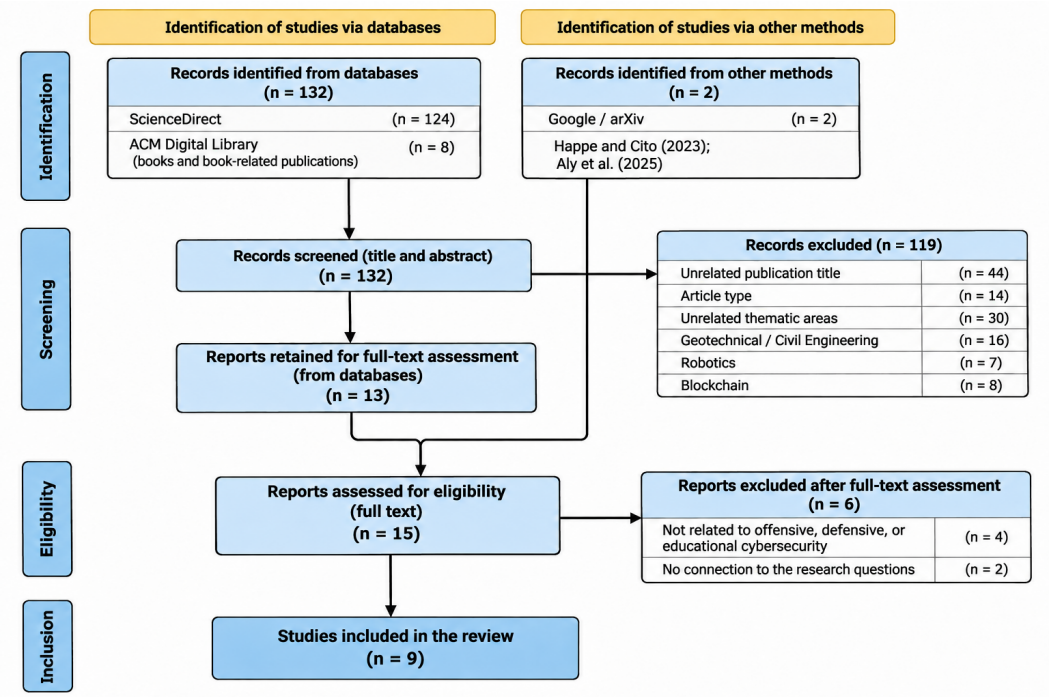


Figure 1. PRISMA 2020-informed flow diagram illustrating study identification through database searches and supplementary sources, screening, full-text eligibility assessment, and final inclusion (Aly et al., 2025; Happe & Cito, 2023). Adapted from Page et al. (2021).

Table 1 summarises the nine selected studies according to the dimensions most relevant to the design of MoonPhase, including technological context, cybersecurity orientation, and the nature of their contribution.

The nine studies included in the systematic review were classified according to their primary cybersecurity orientation. Four studies primarily address offensive security, including automated penetration testing, reinforcement-learning-based vulnerability assessment, and the practices of security professionals Happe and Cito (2023); H. P. T. Nguyen et al. (2025); Skandylas and Asplund (2025); Venturi et al. (2024). Three studies focus on defensive

approaches, covering federated-learning security in IoT environments, adversarial machine-learning resilience, and advanced persistent threat detection through audit-log analysis Aly et al. (2025); J.-P. A. Yaacoub et al. (2023); Ziras et al. (2025). The remaining two studies examine educational approaches, including demonstrative cybersecurity workshops in cyber–physical production systems and gamified risk exploration in IT/OT infrastructures De Marchi et al. (2025); Luh et al. (2025). These categories describe the primary emphasis of each study rather than mutually exclusive functionalities.

Table 1. Summary of studies included in the systematic literature review.

Study	Technology Context	Orientation	Main Contribution
Skandylas and Asplund (2025)	Automated penetration testing	Offensive	Proposes ADAPT, a formalised framework for automating penetration-testing activities, including planning and execution in realistic network environments.
Venturi et al. (2024)	DRL-based VAPT environments	Offensive	Evaluates the generalisation of DQN, PPO, and A2C agents to previously unseen hosts and vulnerability configurations.
De Marchi et al. (2025)	Cyber–physical production systems	Educational	Presents demonstrative IT/OT cybersecurity workshops combining practical attack scenarios, risk awareness, and defensive countermeasures.
H. P. T. Nguyen et al. (2025)	Realistic pentesting environments	Offensive	Introduces PenGym, a framework for training reinforcement-learning agents through real penetration-testing actions in automated cyber-range environments.
J.-P. A. Yaacoub et al. (2023)	IoT; federated learning	Defensive	Reviews security and privacy threats affecting federated learning in IoT systems and discusses protection mechanisms and deployment challenges.
Ziras et al. (2025)	Adversarial machine learning	Defensive	Investigates adversarial attacks against machine-learning models and evaluates adversarial training and detection mechanisms for improving robustness.
Luh et al. (2025)	Gamified IT/OT environments	Educational	Presents a serious-game framework supporting adversarial risk exploration and cybersecurity learning in IT/OT infrastructures.
Happe and Cito (2023)	Offensive security practice	Offensive	Examines the working practices and cognitive strategies of penetration-testing professionals, identifying challenges and opportunities for automation.
Aly et al. (2025)	Audit logs; GNNs; LLMs	Defensive	Combines graph-based anomaly detection and language models to reconstruct interpretable narratives of advanced persistent threats.

Although these studies address complementary aspects of cybersecurity, they differ in their emphasis on technical capabilities, portability, and instructional integration. Several primarily investigate security methods or experimental environments rather than portable educational devices. To contextualise these findings, complementary literature on experiential learning, mobile security laboratories, and multidisciplinary cybersecurity education was also considered Hammad et al. (2022); Narain et al. (2025); Peruma et al. (2018); Rege (2015). These additional references were used for pedagogical contextualisation and were not counted among the nine studies selected through the systematic review. Taken together, the literature suggests an opportunity to integrate offensive and defensive functionalities, guided experimentation, explicit learning outcomes, and ethical reflection within a portable instructional platform. This integration constitutes the principal design objective of MoonPhase.

2.2. Educational Approaches in Cybersecurity

The education-oriented studies included in the systematic review, together with complementary research on experiential cybersecurity education, highlight the relevance of guided hands-on practice, authentic scenarios, and structured reflection. These principles informed the pedagogical design of MoonPhase and its integration into the instructional framework presented in Section 4.

Several studies in the cybersecurity education literature highlight the effectiveness of workshops and serious games in promoting cybersecurity competencies. De Marchi et al. report that hands-on workshops using a cyber–physical production system significantly improved participants' understanding of risks and security practices in industrial IT/OT environments De Marchi et al. (2025). Luh et al. explore gamified information security scenarios for IT/OT infrastructures, showing that serious games can increase engagement and support adversarial risk exploration in a controlled manner Luh et al. (2025). Rege argues for multidisciplinary experiential learning to support holistic cybersecurity education that integrates technical, human and organisational dimensions Rege (2015). Other work on mobile security labs and goal-oriented experiential learning similarly emphasises the value of authentic, scenario-based activities for cybersecurity programmes Hammad et al. (2022); Peruma et al. (2018).

These works support the assumption that experiential and game-based approaches can be effective in engineering education, especially when they allow learners to observe and interact with realistic attack and defence scenarios. At the same time, they also show that learners must confront ambiguity, conflicting objectives and ethical dilemmas, rather than only well-structured textbook problems Hammad et al. (2022); Rege (2015). However, most of the reported platforms are either purely virtual or rely on complex cyber ranges, which may limit accessibility in regular undergraduate courses and in institutions with constrained resources Narain et al. (2025). This creates an opportunity for more lightweight, portable solutions that can be deployed in standard laboratories and outreach activities.

2.3. State of the Art in Portable Cybersecurity Devices

The state-of-the-art analysis focused on three representative devices: Flipper Zero, Pwnagotchi and LilyGO T-Embed ESP32 Evilsocket (2023); Flipper Devices Inc. (2023); LilyGO (2023); Silva (2026a). Flipper Zero offers multiple hardware modules and protocols but is primarily oriented towards hobbyist and professional use, with limited structured educational content and no explicit alignment with engineering curricula Dougherty (2025); Flipper Devices Inc. (2023). Pwnagotchi is highly effective for capturing Wi-Fi handshakes but targets a narrow set of functionalities and provides limited support for broader educational scenarios beyond wireless password auditing Evilsocket (2023). LilyGO ESP32 boards are flexible for prototyping and are frequently used in hobbyist and research projects; however, they lack out-of-the-box integration with advanced auditing tools or curricular materials required in higher education contexts LilyGO (2023).

The comparative analysis suggests that no existing device combines, in a single accessible platform, offensive demonstrations, defensive diagnostics and explicit educational content tailored for teaching in engineering programmes Silva (2026a). MoonPhase was therefore planned to combine and extend the capabilities of these devices, while being explicitly designed as a teaching and demonstration tool. In addition, MoonPhase is intended to be replicable in academic settings, with open designs and supporting materials that lower the barrier for instructors who wish to integrate experiential cybersecurity activities into their courses Silva (2026b).

3. MoonPhase Device

3.1. Overview

MoonPhase is a portable device (see Figure 2) designed for practical experimentation in cybersecurity, integrating multiple modules for the analysis, emission and manipulation of wireless signals in a compact and autonomous form factor Silva (2026b). Its architecture was conceived not only to aggregate technical capabilities, but also to support guided educational activities in which students can observe, execute and discuss cybersecurity phenomena in a controlled setting.

The prototype supports operations such as on–off keying (OOK) signal capture and replay, frequency scanning, packet sniffing, fake access point creation and experimental Bluetooth jamming, while offering an accessible menu-based interface that can be operated without external peripherals. In contrast to hobbyist-oriented tools such as Flipper Zero or Pwnagotchi Evilsocket (2023); Flipper Devices Inc. (2023), MoonPhase was designed from the outset as an educational artefact, with its functionality mapped to learning outcomes and teaching activities in engineering programmes.

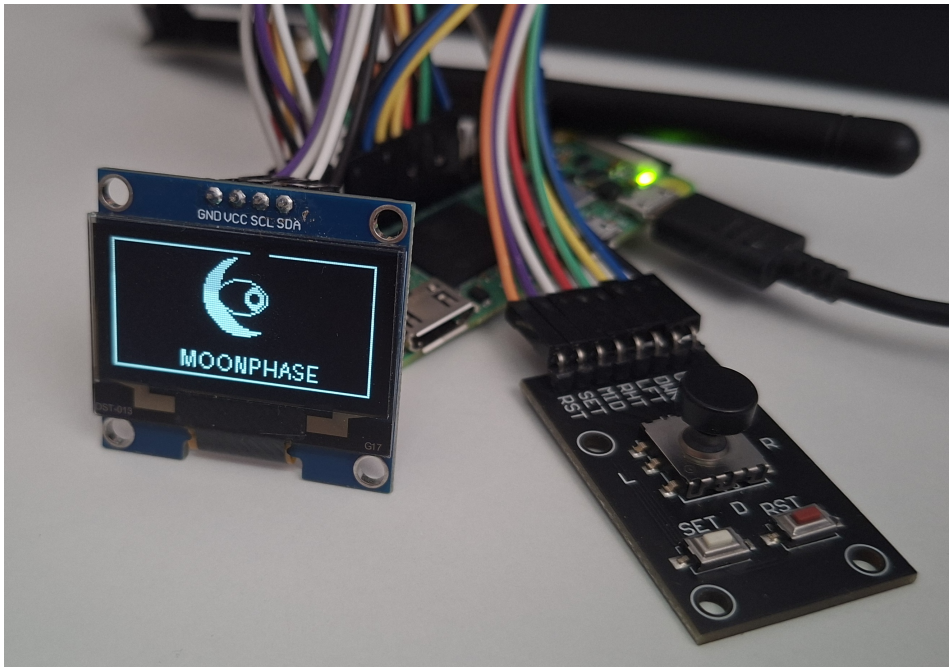


Figure 2. MoonPhase prototype, showing the Raspberry Pi Zero 2 W, OLED display, D-Pad and RF/IR modules in a portable form factor.

The development followed an iterative prototyping methodology that allowed each hardware component and software module to be validated prior to final integration Silva (2026b). Tests conducted in dedicated laboratory scenarios, using controlled networks and test devices, indicate that MoonPhase can operate reliably from a technical standpoint and that it is a plausible candidate for teaching and experimentation on wireless protocols and device behaviour under adverse conditions. This section summarises the hardware and software architecture of the device and its main modes of operation, with particular emphasis on how the main design decisions support portability, guided experimentation, observability of cybersecurity phenomena, and supervised educational use.

3.2. Hardware Architecture

The hardware architecture of MoonPhase is organised into three main layers, as illustrated in Figure 3: interface and control, radio-frequency (RF) communication and infrared

communication Silva (2026b). A Raspberry Pi Zero 2 W acts as the central processing unit, coordinating interactions between the user interface, RF modules and support tools. The choice of a Raspberry Pi platform reflects the widespread use of similar single-board computers in cybersecurity experiments and portable training devices Phuong et al. (2023); E. Yaacoub et al. (2023).

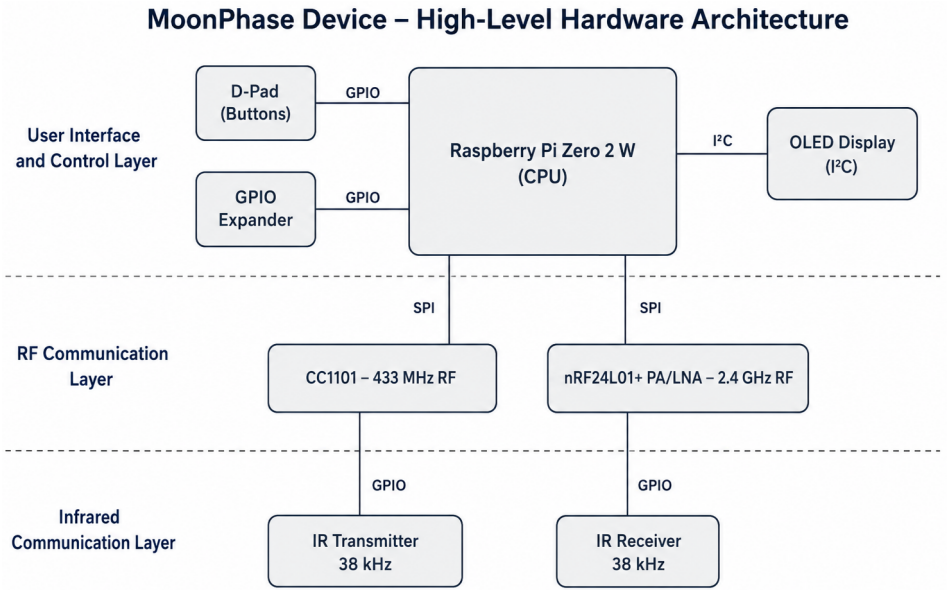


Figure 3. High-level architecture of the MoonPhase device, highlighting the interface and control layer, RF communication layer and infrared communication layer.

The interface and control layer includes the following:

- a 1.3″ OLED display based on the SH1106 controller, connected via I^2C, used to present menus, system states, scan results and other real-time information;
- a D-Pad consisting of a joystick with five directions (UP, DOWN, LEFT, RIGHT, CENTRE) plus SET and RESET buttons, wired to GPIO pins configured as inputs with internal pull-up resistors to ensure stable readings Silva (2026b).

From an instructional perspective, the integrated display and physical controls allow students to interact directly with the device without requiring an external computer during basic activities. This reduces operational overhead in short laboratory sessions and enables the instructor to focus attention on the observed cybersecurity behaviour rather than on peripheral configuration tasks.

The RF communication layer integrates a CC1101 module and an nRF24L01+ PA/LNA module, both connected via SPI to the Raspberry Pi Zero 2 W Silva (2026b). The CC1101 module is used to capture and reproduce low-complexity modulations such as OOK and amplitude shift keying (ASK) around 433 MHz, enabling replay attacks on simple IoT devices, while the nRF24L01+ PA/LNA module supports experiments in the 2.4 GHz band, including Bluetooth jamming and RF activity scanning. The coexistence of these RF capabilities within the same platform also allows instructors to contrast different classes of wireless vulnerabilities within a single learning sequence Flipper Devices Inc. (2023); LilyGO (2023). For example, students can move from passive observation and scanning to controlled demonstrations of replay and interference, making the relationship between attack mechanisms, observable effects and possible countermeasures more explicit.

The infrared communication layer comprises a Keyestudio KS0027 IR emitter and a KS0026 IR receiver (Shenzhen KEYES Robot Co., Ltd., Shenzhen, China), operating at 38 kHz Silva (2026b). These modules allow MoonPhase to capture and replay IR commands

from common remote controls, supporting the demonstration of replay attacks on consumer devices such as TVs and projectors. Because the effect is immediately observable, IR replay also provides a low-complexity introductory example through which students can understand the basic logic of capture-and-replay attacks before addressing less visible wireless scenarios. A JOY-IT four-port GPIO expander is used to reduce cabling complexity and to facilitate the distribution of GPIO pins among the various modules, which also simplifies assembly and maintenance of devices in a teaching laboratory.

3.3. Software Architecture

The software layer is based primarily on Python 3 scripts running on Raspberry Pi OS Lite, complemented by Bash scripts for system-level tasks and integration with external tools Silva (2026b). Python was chosen for its readability, extensive hardware support libraries and ease of integration with security tools, while Bash is used to orchestrate services such as `hostapd`, `dnsmasq` and web servers in offensive modes. This hybrid approach is consistent with other experiential cybersecurity platforms that build on established open-source tools Narain et al. (2025); T. Nguyen et al. (2024).

The main Python application implements the menu system, handles D-Pad input and updates the OLED display in real time, relying on libraries such as `luma.oled`, `spidev`, `RPi.GPIO`, `smbus`, `RF24` and CC1101-specific wrappers for SPI, GPIO and I^2C communication with the RF modules and display Silva (2026b). Network analysis and auditing capabilities rely on command-line tools such as Nmap, which are invoked from Python or Bash and whose results are parsed and displayed on the OLED. By encapsulating these tools behind a menu-driven interface, MoonPhase makes them accessible to students who may not yet be comfortable with command-line use, while still allowing instructors to expose the underlying commands when appropriate. This layered interaction supports progressive scaffolding: novice students can initially focus on interpreting outputs and understanding attack or defence mechanisms through the menu-driven interface, while more advanced students can inspect the underlying commands, scripts and system configuration as their technical proficiency develops.

The codebase is organised into modular components, each handling a specific concern:

- a user interface module, which manages screen rendering and navigation;
- RF and IR modules, which encapsulate signal capture, replay, scanning and interference routines;
- a network tools module, which wraps calls to Nmap and related utilities.

This modular structure facilitates maintenance and future extensions, while also providing a clear entry point for students interested in studying or adapting individual components as part of project-based learning activities. In this way, the implementation itself can become an object of learning, rather than functioning only as an opaque tool used during demonstrations.

3.4. Functional Modes

MoonPhase was conceptually organised into three modes of operation: offensive, defensive and educational Silva (2026a, 2026b). These modes were defined not only as functional groupings, but also as instructional components intended to support complementary stages of cybersecurity learning: observing and reproducing attack mechanisms, analysing systems from a defensive perspective, and explicitly connecting practical observations with underlying concepts, risks and ethical considerations.

In the offensive mode, the device aggregates functionalities oriented towards demonstrating vulnerabilities, including the following:

- creation of a fake Wi-Fi access point with captive portal for phishing demonstrations, implemented using `hostapd`, `dnsmasq` and a lightweight web server;
- capture and replay of OOK signals in the 433 MHz band, targeting simple IoT devices;
- experimental Bluetooth jamming using the nRF24L01+ PA/LNA module to generate interference in the 2.4 GHz spectrum Silva (2026b).

The defensive mode groups diagnostic and monitoring functionalities such as the following:

- network scanning using Nmap to identify hosts and services in local networks;
- basic logging of scan results and RF activity, intended for later analysis and discussion in class Silva (2026b).

The educational mode provides conceptual explanations related to the other modes, including descriptions of Wi-Fi handshakes, phishing, Bluetooth interference and replay attacks, presented as interactive textual content on the OLED Silva (2026a). This mode is designed to support in situ explanations during demonstrations and to reinforce theoretical concepts via the device itself, in line with experiential learning approaches where conceptual and practical components are tightly interwoven Hammad et al. (2022); Rege (2015).

Together, these modes operationalise the design principles identified in the literature review Luh et al. (2025); Narain et al. (2025); Phuong et al. (2023) and provide the functional basis for the instructional activities described in Section 4. The offensive and defensive modes support controlled observation and experimentation with attack and monitoring mechanisms, whereas the educational mode provides contextual explanations that can be used before, during or after the practical activity. Their combined use is intended to connect technical action, interpretation and ethical reflection within the same learning experience.

4. Instructional Design and Curricular Integration

4.1. Design Principles

This section presents the instructional framework developed to support the use of MoonPhase in engineering education. The framework defines how the device's technical functionalities are connected to learning outcomes, guided activities, assessment, and ethical reflection within an experiential learning sequence. Drawing on findings from the systematic review and from prior work on workshops, mobile labs, serious games, and experiential cybersecurity education, the framework positions MoonPhase within structured learning activities that combine technical investigation, interpretation of observed behaviour, and socio-technical reflection Luh et al. (2025); Peruma et al. (2018); Phuong et al. (2023); Rege (2015). Rather than treating the device as an isolated demonstration tool, the framework specifies how its functionalities can be embedded into a coherent instructional sequence and aligned with intended learning outcomes and assessment. The purpose of this framework is to provide a structured basis for designing, implementing, and evaluating MoonPhase-based learning experiences. Its initial application is examined through the exploratory pilot study reported in Section 5, while broader evaluations across cohorts and institutions remain necessary to assess its educational effectiveness more comprehensively Hammad et al. (2022); Narain et al. (2025).

The instructional framework is organised around three learning outcomes:

- LO1—conceptual understanding: identify and explain common vulnerabilities and attack mechanisms in wireless networks and IoT devices, including fake access points and replay attacks;
- LO2—technical interpretation: execute or observe basic cybersecurity operations, such as network scanning and signal capture, and interpret the resulting information under conditions of incomplete or uncertain evidence;

- LO3—ethical and professional reasoning: analyse the ethical and legal implications of offensive cybersecurity techniques and articulate responsible courses of action in controlled educational and professional contexts.

MoonPhase-based activities follow a five-stage instructional sequence:

1. Conceptual preparation, in which the instructor introduces the relevant cybersecurity concepts, learning outcomes, and ethical boundaries;
2. Demonstration, in which selected attack or defence mechanisms are shown using the MoonPhase device in a controlled environment;
3. Guided investigation, in which students interact with the device or analyse its outputs through structured tasks;
4. Interpretation and reflection, in which students relate observed technical behaviour to vulnerabilities, countermeasures, and real-world implications;
5. Assessment and debriefing, in which learning is evaluated and technical observations are connected to ethical, legal, and professional responsibilities.

The three functional modes of MoonPhase support different but complementary stages of this sequence. The offensive mode enables controlled demonstrations of attack mechanisms; the defensive mode supports observation, scanning, and interpretation of system behaviour; and the educational mode provides contextual explanations that can be used to support conceptual preparation and debriefing. The pedagogical value of the platform therefore lies not in any individual functionality, but in the coordinated use of these modes within a structured learning experience. Table 2 summarises the alignment between MoonPhase functionalities, instructional activities, intended learning outcomes, and the corresponding assessment evidence.

Table 2. Alignment between MoonPhase functionalities, instructional activities, learning outcomes, and assessment evidence.

MoonPhase Functionality	Instructional Activity	Expected Learning	Learning Outcome	Assessment Evidence
Fake Wi-Fi access point	Controlled demonstration and identification of suspicious access-point behaviour	Recognition of phishing and insecure Wi-Fi scenarios	LO1, LO3	Pre-/post-test items and ethical discussion
Nmap network scanning	Guided scan and interpretation of detected hosts and services	Interpretation of network exposure and defensive information	LO2	Practical task and pre/post-test items
OOK capture and replay	Controlled capture and reproduction of a wireless command	Understanding of replay vulnerabilities and lack of authentication	LO1, LO2	Pre-/post-test items and guided explanation
Educational mode	Contextual explanations before and after practical activities	Connection between observed behaviour and underlying cybersecurity concepts	LO1, LO3	Post-session questionnaire and discussion
Ethical debriefing	Discussion of acceptable use, legal constraints, and professional responsibility	Recognition of ethical and legal boundaries	LO3	Ethical-awareness questionnaire items

The proposed use of MoonPhase in engineering courses follows a structured experiential sequence in which students alternate between instructor-led conceptual preparation, controlled demonstrations, guided hands-on investigation, interpretation of technical evidence, and structured reflection. Particular emphasis is placed on debriefing moments in which students connect technical observations with broader issues such as user behaviour,

organisational policies and regulatory frameworks Hammad et al. (2022); Rege (2015). This structure aims to bridge the gap between theoretical content and practical skills, while ensuring that offensive capabilities are always framed within ethical and legal boundaries.

4.2. Integration into Engineering Curricula

MoonPhase is intended to be integrated into modules such as *Introduction to Cybersecurity*, *Computer Networks* or *IoT Systems* in computer engineering and related programmes. Typical prerequisites include basic networking concepts, familiarity with Linux command-line tools and a general introduction to security principles. Instructors can use the device to complement existing laboratory infrastructures or, in resource-constrained contexts, as a lightweight alternative to more complex cyber ranges Narain et al. (2025).

Table 3 presents the 90 min MoonPhase-based learning session that was subsequently used in the pilot evaluation described in Section 5.

Table 3. Structure of the 90 min MoonPhase-based learning session used in the pilot study.

Stage	Duration	Activity	Primary Learning Outcome
1	10 min	Introduction, conceptual recap, learning outcomes, and ethical boundaries	LO1, LO3
2	20 min	Controlled demonstration of a fake Wi-Fi access point	LO1, LO3
3	20 min	Guided Nmap network scanning and interpretation	LO2
4	20 min	Controlled OOK capture and replay demonstration	LO1, LO2
5	20 min	Group discussion, ethical debriefing, post-test, and feedback collection	LO1, LO3

During the pilot session, students first received a short conceptual introduction and were informed of the ethical and legal boundaries governing the activities Silva (2026b). They then observed a controlled fake access-point scenario, performed guided network-scanning tasks using Nmap, and observed an OOK capture-and-replay demonstration. The device's menu system and self-contained interface allow the lab to run without additional peripherals, which simplifies logistics and supports portability between classrooms and labs. By situating MoonPhase-based activities within broader discussions about critical infrastructures, privacy and the societal impact of digital technologies, the device contributes to programme-level objectives related to ethics, sustainability and responsible innovation in engineering European Union Agency for Cybersecurity (2025); Europol (2024). The session concluded with a structured discussion on mitigation strategies, responsible use of offensive tools, and professional responsibility, followed by the post-test and perception questionnaire.

The stages in Table 3 are explicitly aligned with the learning outcomes introduced in Section 4. Stages 1 and 2 mainly address conceptual understanding of wireless security mechanisms and common attack vectors (LO1), while Stage 3 emphasises procedural skills in running scans, capturing signals and interpreting MoonPhase outputs under uncertainty (LO2). Stages 4 and 5 focus on ethical reasoning and professional responsibility, asking students to articulate mitigation strategies, discuss institutional policies and reflect on what constitutes acceptable use of offensive tools in engineering practice (LO3). This explicit mapping supports constructive alignment between activities, assessment and programme-level objectives.

Example Multi-Week Sequence

Beyond single-session use, MoonPhase can be embedded into a short multi-week sequence within an introductory cybersecurity module. Table 4 sketches a four-week progression that gradually moves from highly structured demonstrations to more open-ended,

student-designed activities, in line with recommendations for goal-oriented experiential learning in cybersecurity Hammad et al. (2022); Rege (2015).

Table 4. Example four-week sequence using MoonPhase.

Week	Focus	Main MoonPhase Activities
1	Concepts and demo	Instructor-led demos of scans, fake AP and OOK replay
2	Guided practice	Students follow structured lab scripts in small groups
3	Semi-open tasks	Groups design and execute constrained attack/defence scenarios
4	Reflection and ethics	Reporting, peer discussion and ethical case analysis

In Week 1, MoonPhase is used mainly to visualise key concepts such as wireless handshakes, replay attacks and captive portals, with the instructor controlling the device. Week 2 introduces guided practice, where students execute predefined procedures and interpret MoonPhase outputs under supervision. In Week 3, students work in groups to design their own scenarios within clearly defined constraints; for example, choosing a combination of fake AP, OOK replay and scanning tasks that illustrate a particular threat model. Week 4 is devoted to reporting, peer discussion and ethical case analysis, encouraging students to connect their technical experiments with broader questions about risk, responsibility and professional conduct.

4.3. Workshops and Outreach Activities

Beyond formal courses, MoonPhase can be used in short workshops and outreach events targeting heterogeneous audiences such as high-school students, teachers or IT professionals. Prior work on IT/OT workshops and experiential cybersecurity platforms suggests that hands-on demonstrations with real systems increase understanding and engagement across diverse participant profiles Narain et al. (2025); Phuong et al. (2023). In these settings, the device can be operated by the instructor for live demonstrations of OOK replay, Bluetooth jamming or captive portal phishing, or deployed in small-group stations where participants follow simplified scripts under supervision Silva (2026a, 2026b).

Example outreach scenarios include showing how simple IR or 433 MHz remotes can be cloned, or how insecure public Wi-Fi networks can be exploited using fake authentication pages, followed by discussions on how to recognise and avoid such threats in everyday life. These activities support not only technical skill development but also cybersecurity awareness and digital literacy, which are increasingly recognised as essential competencies for citizens in an age of uncertainty and complexity European Union Agency for Cybersecurity (2025); Pawlicka et al. (2023).

4.4. Risk Management and Ethical Guidelines

Because MoonPhase integrates dual-use cybersecurity capabilities, its instructional use requires explicit operational boundaries, instructor supervision, and compliance with applicable legal and institutional requirements. The instructional framework therefore distinguishes between the technical functionalities available in the prototype and the activities selected for supervised educational use.

In the reported educational pilot, the practical activities were conducted in a teaching laboratory using a dedicated Wi-Fi network established specifically for the instructional session. This network provided a designated experimental environment for the fake access-point and network-scanning demonstrations. The OOK capture-and-replay demonstration involved a 433 MHz radio-frequency remote control used to operate a remotely controlled electrical socket. This setup enabled students to observe the relationship between wireless command transmission and the resulting physical action. The activities were therefore

conducted using a specifically configured network and an identifiable radio-controlled device within the laboratory setting.

The 90 min pilot session reported in Table 3 comprised a controlled fake Wi-Fi access-point demonstration, guided network scanning using Nmap, and an OOK capture-and-replay demonstration, followed by ethical reflection and debriefing Silva (2026b). Experimental Bluetooth jamming, although described as a technical capability of the prototype, was not included in the reported pilot protocol. Consequently, the educational evaluation does not provide evidence concerning the instructional use of this functionality.

For the implementation and replication of MoonPhase-based activities, instructors should establish a clearly defined and authorised experimental scope before conducting any demonstrations. Network scanning should be restricted to explicitly authorised hosts and laboratory networks, while wireless capture-and-replay scenarios should involve dedicated test devices. Fake access-point demonstrations should use controlled environments and synthetic information rather than real credentials. Activities should also avoid collecting unrelated network traffic or personal information Phuong et al. (2023); Rege (2015).

Additional precautions apply to radio-frequency interference capabilities. Such functionalities must not be treated as routine classroom exercises and should only be considered where all applicable regulatory requirements, explicit permissions, and appropriate technical safeguards have been verified. Where these conditions cannot be established, prerecorded observations or offline demonstrations provide safer educational alternatives.

Finally, each instructional session should incorporate an explicit discussion of authorisation, responsible disclosure, privacy, acceptable use, and professional accountability. These safeguards form part of the proposed instructional framework and are intended to ensure that technical experimentation remains aligned with ethical and responsible cybersecurity practice.

5. Pilot Educational Evaluation

5.1. Participants and Study Design

An exploratory one-group pre-test/post-test pilot study was conducted with 21 undergraduate students enrolled in a computing-related degree programme. The participants attended a 90 min MoonPhase-based learning session designed according to the instructional sequence described in Section 4 and summarised in Table 3.

The intervention took place in a teaching laboratory equipped with a Wi-Fi network configured specifically for the educational activities. The practical demonstrations included a fake Wi-Fi access point, guided network scanning, and the capture and replay of wireless commands using a 433 MHz remote control and a radio-controlled electrical socket. These activities formed part of the structured 90 min instructional session described in Table 3.

The pilot was conducted as part of a regular teaching activity within the course. Participants were asked to provide their name or student number solely to match their pre-test and post-test responses, enabling the calculation of individual knowledge gains and paired statistical comparisons. For the research analysis, these personal identifiers were replaced with pseudonymous participant codes (P01–P21). The results are reported in aggregated form, and individual qualitative responses are presented using only these participant codes.

The pilot was designed to provide an initial empirical evaluation of three dimensions associated with the proposed instructional framework: changes in cybersecurity knowledge, perceived authenticity and engagement, and ethical awareness. Given the exploratory nature of the study, the limited sample size, and the absence of a control group, the evaluation was intended to provide preliminary evidence rather than a definitive estimate of the educational effectiveness of MoonPhase.

5.2. Research Questions

The pilot study was guided by the following research questions:

- RQ1: What preliminary changes in cybersecurity knowledge are observed following participation in a MoonPhase-based learning session?
- RQ2: How do students perceive the authenticity and engagement of the MoonPhase-based experiential cybersecurity learning activity?
- RQ3: How do students perceive their ethical responsibilities and the legal constraints associated with the use of offensive cybersecurity tools in a controlled educational setting?

5.3. Instruments

Three complementary instruments were used in the pilot evaluation.

First, cybersecurity knowledge was assessed through a 10-item multiple-choice test, administered before and after the 90 min learning session. The same questions were used in both assessments, with four response options and one correct answer per question. Each correct answer contributed one point to the total score, ranging from 0 to 10. The questions covered wireless cybersecurity topics, including rogue access points, replay attacks, network scanning, WEP vulnerabilities, war-driving, penetration-testing authorisation, dual-use tools, MAC address spoofing, responsible vulnerability disclosure, and WPA2 handshakes. Correct answers were not displayed after the pre-test, whereas the post-test provided the final score, correct answers, and technical explanations. The complete knowledge test and post-session questionnaire, reproduced in their original Portuguese wording, are provided in Appendix B.

Second, a post-session questionnaire included three single-item measures rated on a five-point Likert scale. Perceived authenticity assessed whether the simulated scenarios realistically reflected cybersecurity situations; engagement assessed whether the practical activities maintained students' interest and motivation; and self-reported ethical awareness assessed whether the experience reinforced students' perceptions of ethical responsibility, authorisation, and the risks associated with the use of cybersecurity tools. Each dimension was measured by one item and analysed descriptively. These items were intended to capture participants' immediate perceptions rather than to constitute validated psychometric scales.

Finally, an open-ended question asked participants to identify the main aspect they had learned from the MoonPhase-based activity. The purpose of this question was to complement the quantitative measures with qualitative evidence regarding the aspects of the experience that students considered most meaningful.

All open-ended responses were originally provided in Portuguese. Short excerpts reported in the manuscript were translated into English by the authors.

5.4. Data Analysis

Pre-test and post-test scores were summarised using means and sample standard deviations. Individual knowledge gains were calculated by subtracting each participant's pre-test score from their post-test score. The mean knowledge gain was then calculated across the 21 paired observations.

A paired-samples t-test was used to assess whether the mean within-participant difference was statistically significant. Statistical significance was evaluated at $\alpha = 0.05$ using a two-tailed test. The 95% confidence interval for the mean gain was calculated using the Student's t distribution with $n - 1$ degrees of freedom and the standard error of the paired differences. Effect size was quantified using Cohen's d_z, calculated as the mean paired difference divided by the sample standard deviation of the paired differences.

Questionnaire responses were analysed descriptively using mean scores on the five-point Likert scale for perceived authenticity, engagement, and ethical awareness. Because the pilot involved a small convenience sample and no comparison group, inferential claims were restricted to the within-participant pre–post knowledge comparison, while the questionnaire results were interpreted descriptively.

Responses to the open-ended question were analysed using a descriptive thematic coding procedure conducted by a single researcher. Each response was examined to identify its predominant thematic focus and assigned to one mutually exclusive category. Three themes were identified: (i) conceptual and technical understanding, (ii) authenticity and engagement, and (iii) ethical and professional awareness. The classification was based on the main idea expressed in each response rather than on the presence of isolated keywords. Of the 21 responses, 7 were assigned to each theme (33.3%). No predetermined quotas were imposed on the categories. As coding was performed by a single researcher, no inter-rater reliability assessment was conducted.

The original Portuguese responses, their English translations, and the corresponding thematic assignments are provided in Appendix A to support transparency and reproducibility of the qualitative analysis.

5.5. Results

Table 5 summarises the main quantitative results obtained in the pilot evaluation. The educational findings complement the technical validation previously conducted during Project II, in which MoonPhase was shown to reliably execute its core functionalities, including OOK capture and replay, frequency scanning, packet sniffing, fake access-point creation, and experimental Bluetooth interference Silva (2026b). The results reported below therefore focus specifically on the preliminary educational evaluation of the device and instructional framework.

Table 5. Summary of the pilot educational evaluation ($N = 21$).

Metric	Result
Pre-test score (0–10)	5.86 ± 1.42
Post-test score (0–10)	8.24 ± 1.00
Mean knowledge gain	+2.38 points
Paired-samples t-test	$t(20) = 14.744$
p-value (two-tailed)	$p < 0.001$
Effect size (Cohen's d_z)	3.217
95% CI for mean gain	[2.044, 2.718]
Perceived authenticity (1–5)	4.38
Engagement (1–5)	4.57
Self-reported ethical awareness (1–5)	4.29

5.5.1. Knowledge Gains

As shown in Table 5, the 21 participants achieved a mean pre-test score of 5.86 ± 1.42 on the 0–10 scale. Following the 90 min MoonPhase-based learning session, the mean post-test score increased to 8.24 ± 1.00, corresponding to an average absolute gain of 2.38 points.

A paired-samples t-test confirmed a statistically significant improvement in knowledge scores, $t(20) = 14.744$, $p < 0.001$, with a 95% confidence interval for the mean difference of [2.044, 2.718]. The effect size was large (Cohen's $d_z = 3.217$), indicating a substantial within-participant improvement. These findings provide preliminary evidence of increased understanding of the cybersecurity concepts addressed during the session, including wireless vulnerabilities, replay attacks, network scanning, and fake access-point scenarios. The observed learning gain is consistent with prior research emphasising the

value of guided hands-on and experiential activities in cybersecurity education Hammad et al. (2022); Phuong et al. (2023); Rege (2015).

Given the exploratory one-group design, however, the observed improvement cannot be attributed exclusively to the MoonPhase device independently of the instructional activity as a whole.

5.5.2. Perceived Authenticity and Engagement

Students reported high levels of perceived authenticity and engagement following the activity. As summarised in Table 5, perceived authenticity obtained a mean score of 4.38 out of 5, while engagement achieved the highest mean rating, at 4.57 out of 5.

These results indicate that participants perceived the learning activity as closely connected to realistic cybersecurity situations and reported a high level of involvement during the session. This finding is consistent with experiential cybersecurity approaches in which interaction with realistic systems and scenarios is used to support learner engagement and contextual understanding Hammad et al. (2022); Phuong et al. (2023).

Because these dimensions were measured only after the intervention, the results should be interpreted as descriptive perceptions rather than as evidence of change relative to a baseline or comparison condition.

5.5.3. Ethical Awareness

Self-reported ethical awareness achieved a mean score of 4.29 out of 5, as shown in Table 5. Participants therefore reported a high level of awareness regarding the responsibilities and legal constraints associated with the use of offensive cybersecurity techniques after the activity.

This result is aligned with the instructional design of MoonPhase, in which technical demonstrations are accompanied by explicit discussion of acceptable use, mitigation strategies, legal boundaries, and professional responsibility. Such integration is consistent with approaches to cybersecurity education that emphasise the need to combine technical competence with ethical and socio-technical reasoning Phuong et al. (2023); Rege (2015).

Since ethical awareness was assessed only after the session, this result should not be interpreted as evidence of a measured pre–post increase in ethical awareness.

5.5.4. Qualitative Feedback

The open-ended responses provided additional insight into how students interpreted the MoonPhase-based learning experience. As summarised in Table 6, three recurring themes were identified: conceptual and technical understanding, authenticity and engagement, and ethical and professional awareness. Each theme was represented in 7 of the 21 responses (33.3%).

The first theme concerned the development of conceptual and technical understanding through direct observation and experimentation. Students frequently referred to the value of seeing cybersecurity mechanisms operate in practice rather than encountering them only as theoretical concepts. One participant described how creating a fake access point and observing devices connect to it helped reveal the practical danger of this attack (P05, translated by the authors; see Appendix A). Another participant explained that capturing packets during a replay attack and observing their retransmission helped clarify how the protocol vulnerability worked (P02, translated by the authors; see Appendix A).

The second theme reflected the perceived authenticity and engagement of the activity. Students described the session as resembling a realistic cybersecurity scenario and emphasised the motivational value of interacting with real tools and observing system behaviour directly. One participant noted that the practical component "brought the theory

of protocols and vulnerabilities to life" (P06, translated by the authors; see Appendix A), while another described the activity as providing "a perfect bridge between the theoretical concepts covered in class and the reality of working as a security auditor" (P08, translated by the authors; see Appendix A).

The third theme concerned ethical and professional awareness. Students repeatedly referred to the importance of prior authorisation, legal boundaries, responsible use of offensive tools, and professional conduct. One participant emphasised that "the boundary between ethical hacking and cybercrime lies in consent and the legal framework" (P03, translated by the authors; see Appendix A).

Taken together, the qualitative responses reinforce the quantitative findings by showing that students associated the MoonPhase experience not only with technical learning, but also with realism, active involvement, and ethical reflection.

Table 6. Themes identified in the open-ended student responses ($N = 21$).

Theme	Responses	Main Ideas
Conceptual and technical understanding	7 (33.3%)	Understanding replay attacks, fake access points, network scanning, exposed services, wireless security, packet analysis, and attack sequences
Authenticity and engagement	7 (33.3%)	Realistic scenarios, active experimentation, motivation, connection between theory and practice, confidence, and learning through direct system interaction
Ethical and professional awareness	7 (33.3%)	Authorisation, legal boundaries, responsible use of offensive tools, professional conduct, confidentiality, and defensive purpose

6. Discussion

The pilot study provides preliminary empirical evidence supporting the educational use of MoonPhase within the instructional framework proposed in this work. The results should be interpreted as exploratory, given the limited sample size and the absence of a control group, but they nevertheless offer an initial indication of how students respond to a short, structured cybersecurity learning experience centred on a portable physical device.

With respect to RQ1, the increase in mean knowledge scores from 5.86 ± 1.42 in the pre-test to 8.24 ± 1.00 in the post-test, corresponding to an average gain of 2.38 points, suggests that students improved their understanding of the cybersecurity concepts addressed during the session. The statistically significant pre–post difference ($t(20) = 14.744$, $p < 0.001$), with a large within-participant effect size (Cohen's $d_z = 3.217$), is consistent with prior work showing that guided hands-on and experiential activities can support conceptual learning in cybersecurity education Hammad et al. (2022); Phuong et al. (2023); Rege (2015). However, the present design does not allow the observed gain to be attributed exclusively to MoonPhase, since the intervention combined the device with instructor guidance, demonstration, discussion, and structured reflection.

Regarding RQ2, students reported high levels of perceived authenticity (4.38/5) and engagement (4.57/5). These results indicate that participants perceived the activity as closely connected to realistic cybersecurity situations and reported a high level of involvement during the session. This finding is aligned with experiential cybersecurity approaches that emphasise interaction with realistic systems, authentic scenarios, and observable technical consequences as mechanisms for promoting engagement and contextual understanding Hammad et al. (2022); Narain et al. (2025); Phuong et al. (2023). The physical and portable nature of MoonPhase may contribute to this perception by allowing students to interact with concrete attack and defence mechanisms rather than with purely abstract or simulated

representations. Nevertheless, because authenticity and engagement were measured only after the session, the results should be interpreted as descriptive perceptions rather than as evidence of improvement relative to another instructional approach.

For RQ3, self-reported ethical awareness reached a mean value of 4.29/5. This suggests that participants recognised the responsibilities and legal constraints associated with the use of offensive cybersecurity techniques after the activity. The result is consistent with the instructional design of MoonPhase, in which technical experimentation is explicitly combined with ethical debriefing, discussion of acceptable use, and reflection on professional responsibility. This integration reflects recommendations in cybersecurity education that technical competence should be developed alongside ethical, organisational, and socio-technical reasoning Phuong et al. (2023); Rege (2015).

The qualitative findings further support this interpretation. The open-ended responses converged with the quantitative results across the three dimensions examined in the pilot. Students spontaneously referred to improved understanding of technical mechanisms, the realism and practical value of the learning experience, and the ethical and professional responsibilities associated with offensive cybersecurity tools. This convergence between test performance, self-reported perceptions, and qualitative feedback provides a degree of triangulation within the exploratory study, although the small sample and single-session design require cautious interpretation.

Taken together, the findings suggest that the pedagogical value of MoonPhase does not derive solely from the technical capabilities of the device. Rather, its educational contribution lies in the coordinated use of offensive, defensive, and educational functionalities within a structured instructional sequence that connects conceptual preparation, controlled experimentation, interpretation of technical evidence, and ethical reflection. This alignment between device functionality and instructional intent addresses a limitation identified in many portable cybersecurity tools, which are often technically capable but provide limited pedagogical structure.

The technical validation carried out during Project II complements these educational findings. MoonPhase was previously shown to reliably execute its core functionalities, including OOK capture and replay, frequency scanning, packet sniffing, fake access-point creation, and experimental Bluetooth interference Silva (2026b). The combination of technical reliability, portability, and a menu-driven interface therefore provides a practical basis for deployment in regular laboratory environments. At the same time, the presence of offensive capabilities requires clear ethical guidelines, formal usage policies, and careful supervision to ensure that activities remain within legal and institutional boundaries Phuong et al. (2023); Rege (2015).

Limitations

Several threats to validity should be considered when interpreting the pilot results. First, the one-group pre-test/post-test design does not control for alternative explanations such as instructor influence, novelty effects, or familiarity with the assessment instrument Hammad et al. (2022). In particular, the same ten multiple-choice questions were administered before and immediately after the 90 min learning session. Although correct answers were not disclosed following the pre-test, participants may have remembered the questions or response options, potentially contributing to the observed score improvement. Consequently, the measured knowledge gain cannot be attributed exclusively to learning induced by the MoonPhase-based activity. Second, the study involved a small convenience sample from a single educational context, limiting the generalisability of the findings. Third, perceived authenticity, engagement, and ethical awareness were assessed using single-item post-session self-report measures, which may be affected by response

bias, short-term enthusiasm, and limited measurement reliability. Finally, the instruments used in this exploratory study were intended primarily for formative evaluation and were not independently validated as psychometric measures.

Future evaluations should therefore involve larger cohorts, comparison conditions, and repeated deployments across different courses or institutions. More robust designs could compare MoonPhase-based activities with traditional laboratory exercises or virtual-only environments, while retaining equivalent learning objectives and assessment criteria. Replication across contexts, transparent reporting of contextual factors, and triangulation of quantitative and qualitative evidence would help strengthen the external and construct validity of subsequent studies European Union Agency for Cybersecurity (2025); Europol (2024); Narain et al. (2025).

Because the pilot was embedded in a regular teaching activity, the observed outcomes reflect the combined effect of the instructional session, instructor guidance, and use of the MoonPhase platform, rather than the isolated effect of the device.

7. Conclusions and Future Work

This paper has presented MoonPhase, a multifunctional portable cybersecurity device designed to support experiential learning in engineering education. Drawing on a structured literature review, with study identification and selection documented using a PRISMA 2020-informed flow diagram, and on two project-based development cycles (Project I and Project II), MoonPhase integrates offensive, defensive, and educational functionalities within a single portable platform Page et al. (2021); Silva (2026a, 2026b). The proposed approach combines practical cybersecurity experimentation, guided instructional activities, and ethical reflection in a format intended for deployment in regular laboratory settings Luh et al. (2025); Phuong et al. (2023).

The paper has described the hardware and software architecture of MoonPhase, its three functional modes and their alignment with learning outcomes addressing conceptual understanding, technical interpretation, and ethical and professional reasoning. It has also presented an instructional framework for integrating the device into structured experiential learning activities, linking conceptual preparation, controlled demonstrations, guided investigation, interpretation of technical evidence, assessment, and ethical debriefing Hammad et al. (2022); Narain et al. (2025); Rege (2015).

The proposed framework was additionally examined through an exploratory pilot study involving 21 undergraduate students. Mean knowledge scores increased from 5.86 ± 1.42 in the pre-test to 8.24 ± 1.00 in the post-test, corresponding to an average gain of 2.38 points. The pre–post difference was statistically significant ($t(20) = 14.744$, $p < 0.001$), with a large within-participant effect size (Cohen's $d_z = 3.217$). Students also reported high levels of perceived authenticity (4.38/5), engagement (4.57/5), and self-reported ethical awareness (4.29/5). These findings provide preliminary empirical support for the educational use of MoonPhase, while the small sample size, single-group design, and absence of a control condition limit causal interpretation.

The technical and educational findings suggest that the contribution of MoonPhase extends beyond the aggregation of cybersecurity functionalities in a portable device. Its main educational value lies in the coordinated use of offensive, defensive, and educational modes within a structured learning sequence that connects technical experimentation with interpretation, mitigation, and ethical reflection. In this sense, MoonPhase is positioned not only as a technical artefact, but also as an instructional resource for experiential cybersecurity education in engineering contexts Hammad et al. (2022); Phuong et al. (2023); Rege (2015).

Future work will focus on three main directions. First, the physical design will be refined through the development of a dedicated enclosure and improved internal wiring

to increase durability, safety and ease of use in educational settings Silva (2026b). Second, the educational package will be expanded with detailed laboratory manuals, interactive educational content and assessment rubrics integrated with the device's "educational" mode, drawing on best practices from experiential cybersecurity platforms and mobile security labs Narain et al. (2025); Peruma et al. (2018). Third, the preliminary educational evaluation will be extended to larger cohorts, different curricular contexts, and, where feasible, multiple institutions. Future studies should incorporate comparison conditions and repeated deployments to more robustly evaluate knowledge gains, engagement, perceived authenticity, and ethical awareness, while reducing the influence of novelty, instructor effects, and local context Hammad et al. (2022); Phuong et al. (2023).

By making both the technical design and instructional framework available, MoonPhase aims to serve as a basis for further projects and derivatives, encouraging the creation of new educational resources and applications around the physical model. In the longer term, such devices and associated learning designs may contribute to a broader ecosystem of portable, experiential tools that support engineering education in an age of uncertainty and complexity.

Author Contributions: Conceptualization, R.L.d.S., L.M.B. and Â.C.M.d.O.; methodology, R.L.d.S. and L.M.B.; software, R.L.d.S.; validation, R.L.d.S. and L.M.B.; formal analysis, R.L.d.S. and Â.C.M.d.O.; investigation, R.L.d.S.; resources, L.M.B.; data curation, R.L.d.S.; writing—original draft preparation, R.L.d.S.; writing—review and editing, L.M.B. and Â.C.M.d.O.; visualization, R.L.d.S.; supervision, L.M.B. and Â.C.M.d.O.; project administration, L.M.B.; funding acquisition, L.M.B. and Â.C.M.d.O. All authors have read and agreed to the published version of the manuscript.

Funding: This work was funded by National Funds through the Foundation for Science and Technology (FCT), I.P., within the scope of the project UIDB/05583/2020 and DOI identifier https://doi.org/10.54499/UIDB/05583/2020.

Institutional Review Board Statement: The exploratory pilot study was conducted as part of a regular undergraduate teaching activity. No prior formal review or approval by an institutional ethics committee was sought or obtained for the research component of this activity. Informed consent was obtained from all participants, and participation in the research was voluntary. Names or student numbers were collected solely to match pre-test and post-test responses and were subsequently replaced with pseudonymous participant codes (P01–P21) for research analysis. Results are reported in aggregated form, and qualitative responses are identified only by participant codes.

Informed Consent Statement: Informed consent was obtained from all participants involved in the study. Participation was voluntary. Names or student numbers were collected solely to match pre-test and post-test responses and were subsequently replaced with pseudonymous participant codes (P01–P21) for research analysis. Individual identities are not disclosed in the manuscript.

Data Availability Statement: The aggregated quantitative results, descriptive and inferential statistics, and thematic analysis summaries supporting the findings of this study are available through the MoonPhase EDU Research Portal at https://luisbarata.pt/MoonPhaseEDU/data.html (accessed on 29 May 2026). The portal also provides access to supporting research materials and the results dashboard. The assessment instruments and selected qualitative responses are included in the appendices of this article. Individual-level participant data and original free-text responses are not publicly available due to privacy considerations and the potential risk of re-identification associated with the small sample size ($n = 21$). Requests for additional data may be addressed to the corresponding author and will be considered subject to applicable ethical and data protection requirements.

Acknowledgments: We would like to thank the Research Centre in Digital Services (CISeD) and the Instituto Politécnico de Viseu for their support. AI tools were used solely to assist with the linguistic revision and refinement of the manuscript and the verification of statistical results during the revision process. The preparation of the PRISMA flow diagram, was supported by OpenAI's ChatGPT 6.1 Sol image-generation tool. No generative AI tools were used to generate or modify the remaining figures,

produce scientific content, or interpret results. The authors reviewed and validated the manuscript and take full responsibility for its content.

Conflicts of Interest: The authors declare no conflicts of interest.

Appendix A. Original Open-Ended Student Responses and Thematic Classification

This appendix presents the original open-ended responses collected from the 21 participants in the pilot study. All responses are reproduced in Portuguese, preserving their original wording and the order of the source records. Participant codes (P01–P21) are used solely to reference individual pseudonymised responses.

The responses were classified by a single researcher according to their predominant thematic focus. Each response was assigned to one of three mutually exclusive categories: conceptual and technical understanding (CT), authenticity and engagement (AE), or ethical and professional awareness (EP).

Appendix A.1. Original Responses and English Translations

The following responses reproduce the Portuguese text from the pilot-study CSV, followed by English translations prepared for this manuscript. Participant codes P01–P21 correspond to the pseudonymous identifiers in that dataset.

P01. Original (PT): "Ver os pacotes a circular em tempo real no Wireshark enquanto o ataque acontecia tornou o processo de comunicação de rede muito mais transparente."
Translation (EN): "Watching packets flow in real time in Wireshark while the attack was taking place made the network communication process much clearer."

P02. Original (PT): "Apanhar os pacotes durante o replay attack e ver a informação a ser retransmitted ajudou-me a consolidar finalmente como funciona a vulnerabilidade no protocolo."
Translation (EN): "Capturing packets during the replay attack and seeing the information being retransmitted finally helped me consolidate my understanding of how the protocol vulnerability works."

P03. Original (PT): "Esta atividade reforçou que o limite entre o hacking ético e o crime informático está no consentimento e no enquadramento legal."
Translation (EN): "This activity reinforced that the boundary between ethical hacking and cybercrime lies in consent and the legal framework."

P04. Original (PT): "A experiência deu-me uma perspetiva muito mais madura sobre os riscos de segurança e o dever de guardar confidencialidade sobre as vulnerabilidades encontradas."
Translation (EN): "The experience gave me a much more mature perspective on security risks and the duty to maintain confidentiality regarding the vulnerabilities found."

P05. Original (PT): "Conseguir criar um fake access point e ver como os dispositivos se ligavam automaticamente fez-me perceber o perigo real deste tipo de ataque de uma forma que nenhum livro conseguiria explicar."
Translation (EN): "Being able to create a fake access point and see how devices connected automatically helped me grasp the real danger of this type of attack in a way that no book could explain."

P06. Original (PT): "A componente prática fez com que a teoria sobre protocolos e vulnerabilidades ganhasse vida; finalmente fez-se 'clique' sobre o porquê de certas configurações existirem."
Translation (EN): "The practical component brought the theory of protocols and vulnerabilities to life; it finally clicked why certain configurations exist."

P07. Original (PT): "Executar o ataque no laboratório ajudou-me a perceber a sequência lógica que um atacante segue, desde a fase de reconhecimento até à exploração."
Translation (EN): "Performing the attack in the laboratory helped me understand the logical sequence an attacker follows, from reconnaissance to exploitation."

P08. Original (PT): "A atividade fez a ponte perfeita entre os conceitos teóricos das aulas e a realidade do trabalho de um auditor de segurança."
Translation (EN): "The activity provided a perfect bridge between the theoretical concepts covered in class and the reality of working as a security auditor."

P09. Original (PT): "Percebi o risco imenso de utilização indevida destas técnicas e como é fácil causar danos se não agirmos com ética estrita."
Translation (EN): "I realised the enormous risk of misusing these techniques and how easy it is to cause damage if we do not act according to strict ethical principles."

P10. Original (PT): "Foi excelente poder 'sujar as mãos' com ferramentas reais em vez de estar apenas a olhar para diapositivos com comandos."
Translation (EN): "It was excellent to be able to get our hands dirty with real tools instead of just looking at slides showing commands."

P11. Original (PT): "A simulação pareceu um desafio do mundo real, o que me deu muito mais confiança para aplicar estes conceitos no futuro profissional."
Translation (EN): "The simulation felt like a real-world challenge, which gave me much more confidence to apply these concepts in my future career."

P12. Original (PT): "A simulação mostrou-me que o objetivo do conhecimento ofensivo deve ser sempre defender e proteger os sistemas, nunca explorar fragilidades alheias."
Translation (EN): "The simulation showed me that the purpose of offensive knowledge should always be to defend and protect systems, never to exploit other people's weaknesses."

P13. Original (PT): "Sentir que estávamos a trabalhar num ambiente que simulava um cenário real de cibersegurança tornou a aula muito mais envolvente e motivadora."
Translation (EN): "Feeling that we were working in an environment simulating a real cybersecurity scenario made the class much more engaging and motivating."

P14. Original (PT): "A abordagem prática permitiu-me errar, ajustar e perceber a mecânica por trás das redes sem fios de forma realista."
Translation (EN): "The practical approach allowed me to make mistakes, adjust my approach, and understand the mechanics behind wireless networks in a realistic way."

P15. Original (PT): "Compreendi claramente a importância da autorização prévia; usar estas ferramentas fora de um ambiente de testes autorizado tem consequências legais graves."
Translation (EN): "I clearly understood the importance of prior authorisation; using these tools outside an authorised testing environment has serious legal consequences."

P16. Original (PT): "Ter acesso a ferramentas ofensivas tão poderosas fez-me refletir sobre a responsabilidade profissional que um especialista em cibersegurança carrega."
Translation (EN): "Having access to such powerful offensive tools made me reflect on the professional responsibility borne by a cybersecurity specialist."

P17. Original (PT): "O scan de rede deixou de ser apenas um comando teórico no terminal; percebi exatamente que portas e serviços ficam expostos e como um atacante os descobre."
Translation (EN): "Network scanning stopped being merely a theoretical command in the terminal; I understood exactly which ports and services are exposed and how an attacker discovers them."

P18. Original (PT): "Fazer a experimentação direta com os mapas de calor de sinal e o rastreio de redes sem fios abriu-me os olhos para os riscos da proximidade física."

Translation (EN): "Experimenting directly with signal heat maps and wireless network tracking opened my eyes to the risks associated with physical proximity."

P19. Original (PT): "Aprende-se muito melhor quando somos nós a tentar resolver o problema e a ver a reação do sistema ao vivo do que numa aula meramente expositiva."
Translation (EN): "We learn much better when we try to solve the problem ourselves and observe the system's response in real time than in a purely lecture-based class."

P20. Original (PT): "Ficou evidente a necessidade de cumprir os protocolos de conduta e as políticas de segurança da organização antes de executar qualquer teste de penetração."
Translation (EN): "The need to comply with codes of conduct and the organisation's security policies before performing any penetration test became clear."

P21. Original (PT): "Identificar na prática as vulnerabilidades do Wi-Fi mostrou-me claramente a diferença entre os diferentes níveis de segurança e encriptação."
Translation (EN): "Identifying Wi-Fi vulnerabilities in practice clearly showed me the differences between the various levels of security and encryption."

Appendix A.2. Thematic Classification

Table A1 presents the thematic assignment of the 21 responses. Classification was based on the predominant meaning expressed in each response. Each response was counted once.

Table A1. Thematic classification of the original open-ended student responses.

Theme	Response IDs	Frequency
Conceptual and technical understanding (CT)	P01, P02, P05, P07, P17, P18, P21	7 (33.3%)
Authenticity and engagement (AE)	P06, P08, P10, P11, P13, P14, P19	7 (33.3%)
Ethical and professional awareness (EP)	P03, P04, P09, P12, P15, P16, P20	7 (33.3%)
Total		21 (100%)

The classification was conducted by a single researcher. Consequently, inter-rater reliability was not assessed. The equal distribution across the three categories reflects the thematic assignments presented above.

Appendix B. Research Instruments

This appendix presents the original assessment instruments used in the MoonPhase pilot study. The instruments were administered in Portuguese.

Appendix B.1. Cybersecurity Knowledge Test

The same ten multiple-choice questions were administered before and after the 90 min learning session. Each question contained four response options and one correct answer. Each correct response was awarded one point, resulting in a total score between 0 and 10. Correct answers were not disclosed after the pre-test.

1. Qual é o principal objetivo de um atacante ao configurar um "Rogue Access Point" ou "Evil Twin" numa rede sem fios?

    A. Aumentar a velocidade de transmissão da rede original.
    B. Interceptar credenciais e tráfego de utilizadores que se conetem julgando ser a rede legítima.
    C. Bloquear fisicamente o sinal de radiofrequência dos routers vizinhos.
    D. Apenas medir a densidade de dispositivos numa determinada área geográfica.

2. Em que consiste um "Replay Attack" no contexto de comunicação sem fios?

   A. Na alteração em tempo real do código-fonte do firmware do ponto de acesso.
   B. Na destruição física das antenas de transmissão para forçar a desconexão.
   C. Na captura de transmissões válidas de dados para posterior retransmissão não autorizada a fim de replicar a autenticação.
   D. Na injeção de vírus diretamente na memória RAM dos smartphones conectados.

3. Qual das seguintes ferramentas é amplamente utilizada para varredura de portas e identificação de serviços numa rede?

   A. Nmap
   B. Aircrack-ng
   C. Wireshark
   D. John the Ripper

4. Por que motivo o protocolo WEP (Wired Equivalent Privacy) é atualmente considerado inseguro?

   A. Porque só funciona em frequências superiores a 6 GHz.
   B. Devido a falhas no vetor de inicialização (IV) e à fraca implementação do algoritmo RC4, permitindo que a chave seja recuperada rapidamente.
   C. Porque exige a instalação de certificados digitais em todos os clientes.
   D. Porque limita o número máximo de utilizadores conectados a apenas três.

5. O que caracteriza a prática de "War-Driving"?

   A. A destruição remota de redes Wi-Fi através do envio de sinais de alta potência.
   B. O ato de circular por uma zona geográfica para detetar e mapear redes sem fios e as suas vulnerabilidades.
   C. O roubo físico de routers de escritórios empresariais.
   D. O envio em massa de e-mails de phishing a partir de um veículo em movimento.

6. Num teste de penetração ético (Penetration Test), o que define os limites do que o auditor pode ou não testar?

   A. A intuição do próprio auditor no momento da execução.
   B. As Regras de Engajamento ("Rules of Engagement") e a autorização explícita e formal por escrito do proprietário dos sistemas.
   C. O tipo de sistema operativo instalado no alvo.
   D. As recomendações informais obtidas em fóruns de discussão na Internet.

7. O que distingue uma ferramenta de segurança de "uso duplo" (dual-use tool)?

   A. Uma ferramenta que só pode ser instalada em dois computadores em simultâneo.
   B. Uma ferramenta que pode ser utilizada tanto para fins legítimos de diagnóstico/defesa como para atividades maliciosas de ataque.
   C. Um software que funciona obrigatoriamente em Linux e Windows ao mesmo tempo.
   D. Um programa que exige duas palavras-passe para ser executado.

8. Qual é o objetivo da técnica de "MAC Address Spoofing" em redes Wi-Fi?

   A. Aumentar o alcance do sinal da placa de rede sem fios.
   B. Alterar a chave de encriptação WPA2 durante a transmissão.
   C. Mascarar o endereço físico real da placa de rede, assumindo a identidade de um dispositivo autorizado para ultrapassar filtros de rede.
   D. Desativar permanentemente o router da vítima.

9. Qual é a conduta ética correta após a descoberta de uma vulnerabilidade num sistema durante um laboratório autorizado?
   A. Publicar imediatamente os detalhes da falha nas redes sociais para alertar o público.
   B. Vender a informação sobre a falha no mercado negro.
   C. Registar a vulnerabilidade e comunicá-la responsavelmente aos responsáveis do sistema ("Responsible Disclosure") através de um relatório técnico.
   D. Usar a falha para apagar os registos de log do servidor.
10. O que proporciona o mecanismo de "Handshake de 4 vias" (4-Way Handshake) no protocolo WPA2?
   A. Permite a troca rápida de ficheiros multimédia entre computadores.
   B. Garante a autenticação mútua e estabelece chaves de encriptação temporárias sem nunca transmitir a palavra-passe original na rede.
   C. Desativa a necessidade de utilizar palavras-passe em redes empresariais.
   D. Cria uma cópia de segurança automática de todos os dados do utilizador.

key:

1–B; 2–C; 3–A; 4–B; 5–B; 6–B; 7–B; 8–C; 9–C; 10–B.

Appendix B.2. Post-Session Perception Questionnaire

Following the knowledge post-test, participants completed a short questionnaire comprising three single-item measures and one open-ended question. Each quantitative item was rated on a five-point scale, from 1 to 5. The original Portuguese wording is reproduced below.

1. Autenticidade Percebida: A atividade e os cenários simulados refletiram de forma realista situações reais de cibersegurança? 1 (Pouco realista) to 5 (Muito realista).
2. Envolvimento (Engagement): A realização prática dos testes/laboratório manteve o seu interesse e motivação durante a aula? 1 (Baixo) to 5 (Muito Alto).
3. Consciência Ética e Legal: Esta experiência reforçou a sua perceção sobre a responsabilidade ética, autorização e riscos do uso destas ferramentas? 1 (Pouco reforçado) to 5 (Muito reforçado).

Open-ended question:

Partilhe com as suas palavras o que aprendeu ou achou mais relevante na atividade prática:

The open-ended responses were analysed using the descriptive thematic coding procedure described in Section 5.4. The original responses, English translations, and thematic assignments are provided in Appendix A.

Appendix C. Systematic Literature Review Protocol

This appendix provides additional methodological details on the literature review conducted during Project I, which informed the design and instructional positioning of MoonPhase. The information presented here is based on the original project report Silva (2026a).

Appendix C.1. Review Questions

The review was guided by four questions:

- RQ-SLR1: How can ESP32- or Raspberry Pi-based devices contribute to network auditing and security testing?

- RQ-SLR2: Which hardware and software technologies are commonly used in portable cybersecurity devices?
- RQ-SLR3: What role does cybersecurity play in educational and training environments?
- RQ-SLR4: What advances have been reported in multifunctional devices supporting offensive and defensive cybersecurity activities?

These questions guided the identification of technical, functional, and educational characteristics relevant to the development of MoonPhase.

Appendix C.2. Search Strategy

The primary database search was conducted on 25 October 2025 using ScienceDirect and the ACM Digital Library. The original researcher reported using the following Boolean search expression:

```
"penetration testing" OR "ethical hacking" OR
"security auditing" AND
("Raspberry Pi" OR "portable device" OR "ESP32")
AND ("Wi-Fi" OR "Bluetooth")
AND ("education" OR "training" OR
"learning environment")
```

The expression is reproduced as reported by the researcher, without retrospectively modifying its Boolean structure. Its execution was adapted to the search interfaces available on the respective platforms.

ScienceDirect was used primarily to identify research articles relevant to cybersecurity technologies and educational applications. In the ACM Digital Library, an initially broad search was subsequently restricted to books and book-related publications to complement the article-oriented search performed through ScienceDirect.

The searches considered the 2020–2025 publication period. English and Portuguese were the eligible publication languages. The database searches were complemented by targeted searches using Google, which led to the identification of two preprints available on arXiv: Happe and Cito (2023) and Aly et al. (2025). Their formally published ACM proceedings versions were used as bibliographic references in the final manuscript.

The use of supplementary identification methods was intended to capture relevant contributions that were not retrieved through the selected database searches.

Appendix C.3. Eligibility Criteria

The inclusion criteria documented for the review were:

1. Publication between 2020 and 2025;
2. Publication in English or Portuguese;
3. Relevance to portable devices applied to cybersecurity;
4. Coverage of wireless technologies, cybersecurity education, training, or related learning environments.

Studies were excluded when they fell outside the specified publication period, were unrelated to cybersecurity, lacked a relevant connection to portable technologies or the review questions, or did not contribute to the analysis of cybersecurity tools, technologies, or approaches.

Appendix C.4. Study Selection

The database searches identified 132 records, comprising 124 from ScienceDirect and eight from the ACM Digital Library.

No duplicate removals were reported during the original screening process. Accordingly, all 132 database records were included in the reported title and abstract screening stage.

During screening, 119 records were excluded. The documented exclusion categories were as follows:

- Unrelated publication titles ($n = 44$);
- Publication type ($n = 14$);
- Unrelated thematic areas ($n = 30$);
- Geotechnical or civil engineering topics ($n = 16$);
- Robotics ($n = 7$);
- Blockchain ($n = 8$).

Following these exclusions, 13 database-derived reports remained eligible for full-text assessment.

Two additional reports were identified through supplementary Google searches and retrieved from arXiv: Happe and Cito (2023) and Aly et al. (2025). These reports were not part of the 132 records initially retrieved from the databases. Consequently, 15 reports underwent full-text eligibility assessment, comprising 13 database-derived reports and two reports identified through supplementary searches.

Six reports were excluded after full-text assessment: four exclusions as unrelated to offensive, defensive, or educational cybersecurity and two as insufficiently connected to the review questions. Nine studies were retained for the final synthesis. The corresponding identification and selection process is illustrated in Figure 1.

Appendix C.5. Data Extraction and Synthesis

For the nine included studies, information was organised according to bibliographic identification, publication year, technological context, and primary cybersecurity orientation (offensive, defensive, or educational).

The synthesis was descriptive and focused on identifying the technical and instructional characteristics relevant to MoonPhase. Particular attention was given to the relationship between cybersecurity functionalities, portable hardware, practical experimentation, and educational integration.

The included studies and their main contributions are summarised in Table 1.

References

Aly, A., Mansour, E., & Youssef, A. (2025). OCR-APT: Reconstructing APT stories from audit logs using subgraph anomaly detection and LLMs. In *Proceedings of the 2025 ACM SIGSAC conference on computer and communications security* (pp. 261–275). Association for Computing Machinery. [CrossRef]

De Marchi, M., Pomalo, M., Vallazza, R., Falcomatà, I., Aruväli, T., & Rauch, E. (2025). Enhancing IT/OT Cybersecurity knowledge transfer through demonstrative workshops in cyber-physical production systems. *Procedia Computer Science*, *253*, 2296–2305. [CrossRef]

Dougherty, D. (2025). *Hacking the planet from your pocket*. Available online: https://makethings.make.co/p/hacking-the-planet-from-your-pocket (accessed on 21 May 2026).

European Union Agency for Cybersecurity. (2025). *Enisa threat landscape 2025* (Tech. Rep.). ENISA. Available online: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025 (accessed on 21 May 2026).

Europol. (2024). *Internet organised crime threat assessment (iocta) 2023* (Tech. Rep.). European Union Agency for Law Enforcement Cooperation. Available online: https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2023 (accessed on 21 May 2026).

Evilsocket. (2023). *Pwnagotchi: Deep reinforcement learning WI-FI hacking*. Available online: https://pwnagotchi.ai/ (accessed on 21 May 2026).

Flipper Devices Inc. (2023). *Flipper zero documentation*. Available online: https://docs.flipperzero.one/ (accessed on 21 May 2026).

Hammad, E., Nelson, J., & Romero, J. (2022). Towards goal-oriented experiential learning for cybersecurity programs. In *2022 ASEE annual conference & exposition*. ASEE . [CrossRef]

Happe, A., & Cito, J. (2023). Understanding hackers' work: An empirical study of offensive security practitioners. In *Proceedings of the 31st ACM joint european software engineering conference and symposium on the foundations of software engineering* (pp. 1669–1680). Association for Computing Machinery. [CrossRef]

LilyGO. (2023). *T-embed esp32 board and open-source repository*. Available online: https://github.com/Xinyuan-LilyGO (accessed on 21 May 2026).

Luh, R., Eresheim, S., Tavolato, P., Petelin, T., Gmeiner, S., Holzinger, A., & Schrittwieser, S. (2025). Gamifying information security: Adversarial risk exploration for IT/OT infrastructures. *Computers & Security*, *151*, 104287. [CrossRef]

Narain, S., Rayavaram, P., Morales-Gonzalez, C., Harper, M., Abbasalizadeh, M., Vellamchety, K., & Fu, X. (2025). Practical cybersecurity education: A course model using experiential learning theory. In *Proceedings of the 56th ACM technical symposium on computer science education* (Volume 1, pp. 819–825). Association for Computing Machinery. [CrossRef]

Nguyen, H. P. T., Hasegawa, K., Fukushima, K., & Beuran, R. (2025). PenGym: Realistic training environment for reinforcement learning pentesting agents. *Computers & Security*, *148*, 104140. [CrossRef]

Nguyen, T., Chen, Z., Hasegawa, K., Fukushima, K., & Beuran, R. (2024). PenGym: Pentesting training framework for reinforcement learning agents. In *Proceedings of the 10th international conference on information systems security and privacy—ICISSP* (pp. 498–509). SciTePress. [CrossRef]

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., ...Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ*, *372*, n71. [CrossRef] [PubMed]

Pawlicka, A., Tomaszewska, R., Krause, E., Jaroszewska-Choraś, D., Pawlicki, M., & Choraś, M. (2023). Has the pandemic made us more digitally literate? *Journal of Ambient Intelligence and Humanized Computing*, *14*(11), 14721–14731. [CrossRef] [PubMed]

Peruma, A., Malachowsky, S., & Krutz, D. (2018). Providing an experiential cybersecurity learning experience through mobile security labs. In *2018 IEEE/ACM 1st international workshop on security awareness from design to deployment (SEAD)* (pp. 51–54). IEEE. [CrossRef]

Phuong, C., Saied, N., & Yang, L. (2023). A hands-on education framework for cybersecurity. In *2023 IEEE frontiers in education conference (FIE)* (pp. 1–5). IEEE. [CrossRef]

Rege, A. (2015). Multidisciplinary experiential learning for holistic cybersecurity education, research and evaluation. In *Proceedings of the 2015 USENIX summit on gaming, games, and gamification in security education (3GSE)*. USENIX Association. Available online: https://www.usenix.org/conference/3gse15/summit-program/presentation/rege (accessed on 21 May 2026).

Silva, R. L. d. (2026a). *Desenvolvimento de dispositivo portátil multifuncional para cibersegurança: Perspetiva ofensiva, defensiva e educativa—projeto I* (Project I report). Escola Superior de Tecnologia, Instituto Politécnico de Castelo Branco.

Silva, R. L. d. (2026b). *Desenvolvimento de dispositivo portátil multifuncional para cibersegurança: Perspetiva ofensiva, defensiva e educativa—projeto II* (Project II report). Escola Superior de Tecnologia, Instituto Politécnico de Castelo Branco.

Skandylas, C., & Asplund, M. (2025). Automated penetration testing: Formalization and realization. *Computers & Security*, *155*, 104454. [CrossRef]

Venturi, A., Andreolini, M., Marchetti, M., & Colajanni, M. (2024). Assessing generalizability of deep reinforcement learning algorithms for automated vulnerability assessment and penetration testing. *Array*, *24*, 100365. [CrossRef]

Yaacoub, E., Al-Asaad, H., Salloum, G., & Sharafeddine, S. (2023). Lightweight security mechanisms for federated learning in IoT systems. *IEEE Internet of Things Journal*, *10*(18), 16245–16258. [CrossRef]

Yaacoub, J.-P. A., Noura, H. N., & Salman, O. (2023). Security of federated learning with IoT systems: Issues, limitations, challenges, and solutions. *Internet of Things and Cyber-Physical Systems*, *3*, 155–179. [CrossRef]

Ziras, G., Farao, A., Zarras, A., & Xenakis, C. (2025). From vulnerability to resilience: Adversarial training and real-time detection for AI security. *Array*, *28*, 100546. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.