Minigma – A compact tool for cyber education

Chris Lowerson
School of Computing &
Communications
Lancaster University
Lancaster, UK
c.lowerson@lancaster.ac.uk

This paper presents the concept for Minigma – a compact cyber toolkit designed to serve as a physical, tangible aid for cyber security awareness, education, and engagement. Minigma functions both as an interactive learning tool and as a playful artefact that gamifies core cyber security principles. It aims to bridge the knowledge gap by offering learners a hands-on, accessible and demystifying experience with common cyber tools and techniques. Its primary use case is as a portable engagement resource to be deployed in schools, community groups, and entry-level security awareness workshops.

I. Introduction / Background (Sytle: Heading 1)

As the world embraces more and more digital technology, cyber security awareness remains a critical gap in digital literacy across public and private sectors, at all ages and levels. Minigma is proposed as a hands-on mini toolkit embedded with core cyber security concepts and tools around encryption and decryption. Minigma aims to introduce users to core ideas such as password cracking, encryption, decryption, and steganography via tactile mini-games and microtools. This would be the first digital device to form part of a wider ambition to create a full-suite solution in the form a "Cyber Escape Room", where this device would be one of multiple ways of engaging and leading users through a series of puzzles and digital devices. Minigma fits in the palm of the hand, but opens up layers of digital literacy through curiosity-led discovery.

II. Related Work

Existing tools that combine physical play with digital concepts include escape rooms, cyber security card games, and kits like the **BBC Micro:bit**. The **Cyber Security Escape Co.**[1] and games like **Turing Tumble** and **Piper Computer Kit** similarly blend hands-on learning with digital skills. Minigma builds on this concept by providing a condensed, low-cost and transportable kit that gives user a tangible device to encourage experimentation and aims to go beyond a standard tablet or phone as an interface. Additionally, its design is informed by gamification literature in cyber education [1][2] and draws on research around embodied learning and physical computing [3].

III. Imagined or existing prototype sketches/drawings/photos

A – Prototype description:

The Minigma toolkit is imagined as a modular device, roughly the size of a small external hard drive (approx. 10cm x 6cm), consisting of:

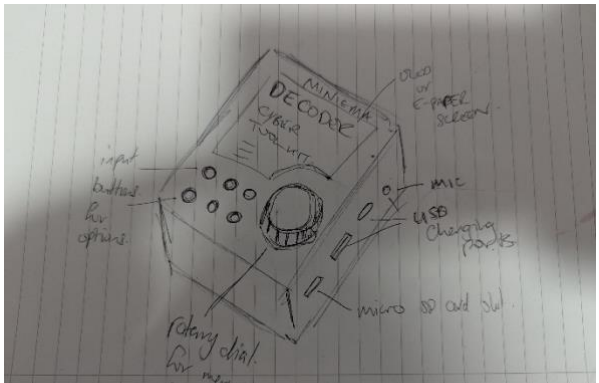
- **Microcontroller (e.g. Arduino Nano or ESP32):** to handle I/O functions, and act as the core controller.
- **OLED Display:** small, low-energy display for running terminal-style messages and simulated command-line interfaces.
- **Rotary Encoder & Buttons:** for navigating through menus and controlling mini-games.
- **Micro-SD Card Reader:** to load custom content or save 'logs' from completed puzzles.
- **Raspberry Pi Pico / RP2040:** optional secondary brain for handling more complex logic games or external connections to future devices/segments.
- **Battery-powered or USB-C powered for portability.**

B – Embedded Challenges

Each hardware component is paired with a 'challenge' or interaction:

- **Password Cracking Puzzle:** Users are given clues to brute-force or social engineer a password using logic and deduction.
- **Steganography Station:** The OLED displays an image that hides a text string, which can be extracted using clues.
- **Encryption/Decryption Game:** A Caesar cipher dial, built physically with rotary input, allows users to decode messages.

C – Initial Concept Sketch:



[1] https://www.cyberescaperoom.co/#

IV. Responsible innovation

Minigma is designed with accessibility and ethics in mind. As a non-invasive, non-networked device, it avoids creating security vulnerabilities. By relying on open-source hardware and software, it maintains transparency. The modular design encourages repairability and reusability. Environmentally, parts are chosen for low power draw and recyclability. Socially, the device is intended to empower and engage learners, especially those excluded from traditional STEM education pathways. The use of gamified and story-led challenges seeks to create engaging, low-stakes ways of understanding serious cyber topics.

V. Author bio(s) / experiences

Chris Lowerson is a Partnerships Development Manager within Lancaster University's School of Computing and Communications. With a background in entrepreneurship, education, and cyber innovation, Chris has previously designed Black Swan an Intellectual Property (IP) educational board game; run the Greater Manchester Cyber Foundry (GMCF) and delivered countless workshops on cyber security awareness. Most recent project is "Hexventure" – a cyber entrepreneurship game aimed at Key Stages 3~5 to encourage users to use entrepreneurial thinking as part of the problem solving, in a cyber security context. Chris is passionate about playful technology, responsible innovation and bridging the divide between technical research and public engagement.

VI. Acknowledgements

Black Swan was a funded project through the UK Intellectual Property Office; GMCF was part-funded by the European Regional Development Framework and a consortium of Manchester Metropolitan University, Lancaster University, Manchester University, and Salford University; Hexventure was funded as a project through the National Cyber Security Centre. This work was inspired by collaboration with NW Regional Organised Crime Unit. Thanks to the Lancashire Constabulary cyber engagement team for continued support, and to the National Cyber Security Centre for outlining accessible cyber principles. Special thanks to colleagues from LU and the Knowledge Exchange community who helped refine the concept at early stages.

VII. Refernces

[1] Marciano, V., du Toit, J., Maluleka, R. (2025). Gamification in Cybersecurity Training: High-Level Properties of Cybersecurity Games. In: Clarke, N., Furnell, S. (eds) Human Aspects of Information Security and Assurance. HAISA 2024. IFIP Advances in Information and Communication Technology, vol 722. Springer, Cham. https://doi.org/10.1007/978-3-031-72563-0_6

[2] Buckley, Tash; Buckley, Oliver (2024). Cracking the code: a cyber security escape room as an innovative training and learning approach. Loughborough University. Conference contribution. https://hdl.handle.net/2134/28525835.v1

[3] Moyosore Ale, Miriam Sturdee, Elisa Rubegni, A systematic survey on embodied cognition: 11 years of research in child–computer interaction, International Journal of Child-Computer Interaction, Volume 33, 2022, 100478, ISSN 2212-8689,

https://doi.org/10.1016/j.ijcci.2022.100478.

- - - - - - - -