Open Access License Notice

Reframing Cyber Security for the Next Generation of Digital Activists

Joe Reddington
Information Security Group
Royal Holloway, University of London
Egham, TW20 0EX, UK
j.reddington@rhul.ac.uk
0009-0007-4268-3347O

Elizabeth A. Quaglia
Information Security Group
Royal Holloway, University of London
Egham, TW20 0EX, UK
e.quaglia@rhul.ac.uk
0000-0002-4010-773X

Abstract—This paper presents a novel short course on cyber security designed for secondary school students in the UK. Our approach uniquely frames cyber security within the context of social activism and change-making, aiming to broaden participation and break down entry barriers in the field. The course contextualizes standard cyber security concepts such as information management, privacy, threat modeling, and cryptography within scenarios relevant to young activists.

We developed comprehensive lesson plans, interactive activities, and tools like "Change Cards" to facilitate engagement. The course was tested in two educational settings, leading to insights about content delivery and student engagement. Key outcomes include a teacher's guide and professionally designed resources that have been downloaded by over 1,000 teachers worldwide.

Feedback from students and teachers has been overwhelmingly positive, highlighting the course's relevance to daily life and its effectiveness in improving understanding of security concepts. This project contributes to the field by offering an innovative approach to cyber security education that resonates with young people's desire for social change, potentially fostering a new generation of diverse cyber security advocates and professionals.

Keywords—*Cyber Security, Diversity, Social Activism*

I. INTRODUCTION

The majority of young people have only the most basic concepts of cyber security [1]. Even in the 16-18 age group, a time when young people are starting to express themselves, explore relationships, and navigate their own personal privacy, the education sector is largely lacking. Worse, when advice or guidance is given, it typically comes in the form of "share nothing, put nothing on social media, protect your privacy at all costs", which is too restrictive and draconian to be accepted by young people finding their place in the world.

This is despite the fact that young people face more cyber risks than any generation before them: online abuse, doxing, and other threats are common, salient, and damaging [2]–[5]. There is a clear and present need to prepare students to build a resilient cyber culture.

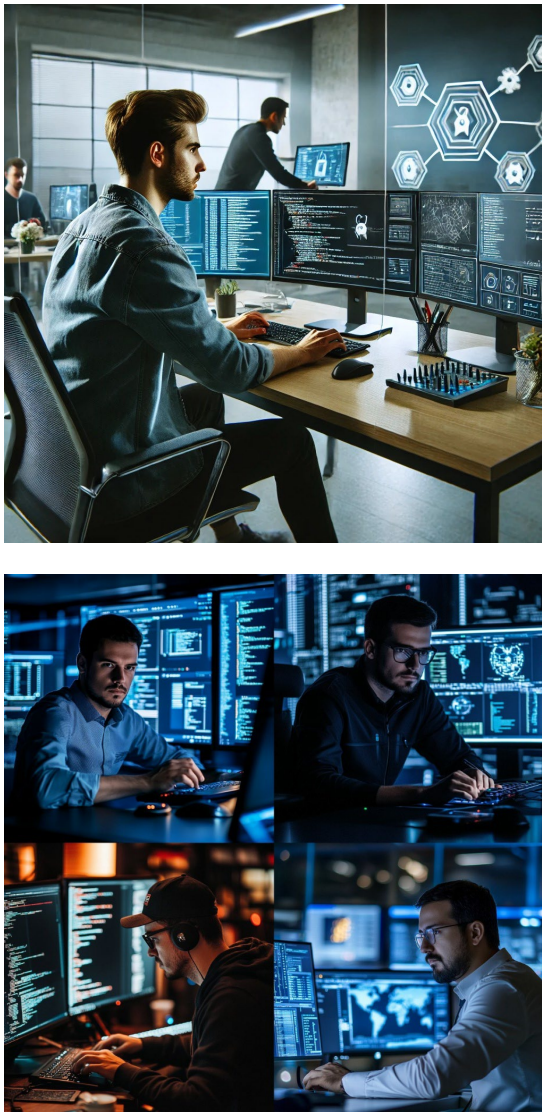

Fig. 1. What cyber security professionals look like according to (top) ChatGPT [10] and (bottom) Midjourney. [11]

Part of the disconnect is caused by the very image of 'cyber security', which is seen as about control and cryptography and has a clear image in the cultural zeitgeist (Figure 1 shows how AI image generators think a cyber security professional looks).[1] This raises the question: can we 'rebrand' the topic in a way that is much more accessible to young people, particularly those most at risk?

A. Our Concept

Our idea is to use an innovative approach to cyber security education (similar to [8]) by developing resources and delivering a short course targeted precisely at young adults who don't think that the classic image of cyber security relates to them or their lives.

To select a cohort of young people for our project, the following questions were key:

- Which groups of young people are most at risk from digital harm?
- Which groups of young people are least likely to identify with the standard 'image' of cyber-security?

After a short process, we selected *digital activists*, which we define as young people with a strong motivation to make a change in society. Those young people that are interested in changing the world are often exactly the ones that are most at risk from bad actors and would benefit from more cyber security knowledge and training but they are also exactly the ones that don't identify with the cultural stereotype. Members of this category are strongly motivated and technologically active, but mostly lack the education and awareness of the security and privacy threats and impact of their digital choices.

The selection of this group felt particularly natural because activists of all types work in a context of constantly shifting assessments of risk and within dynamically forming and reforming groups [5], [9]. Moreover, activists are constantly having to make trade-offs between their personal privacy and their ability to influence events. The world that these young people inhabit, or want to inhabit, is extremely rich in interesting cyber security examples. It is our belief that by offering these students information on 'achieving successful safe social change' we can gain vastly better educational outcomes than if we offered information on cyber security.

As a bonus, by producing materials for students interested in social change, we naturally select for community-focused individuals with strong leadership, and so the potential for them to share good practices in cyber security with others is quite high.

We developed a theory of change [12] to clarify the envisaged hierarchy of changes within the project from the immediate results of activities to long term impacts. This can be seen in Figure 2.

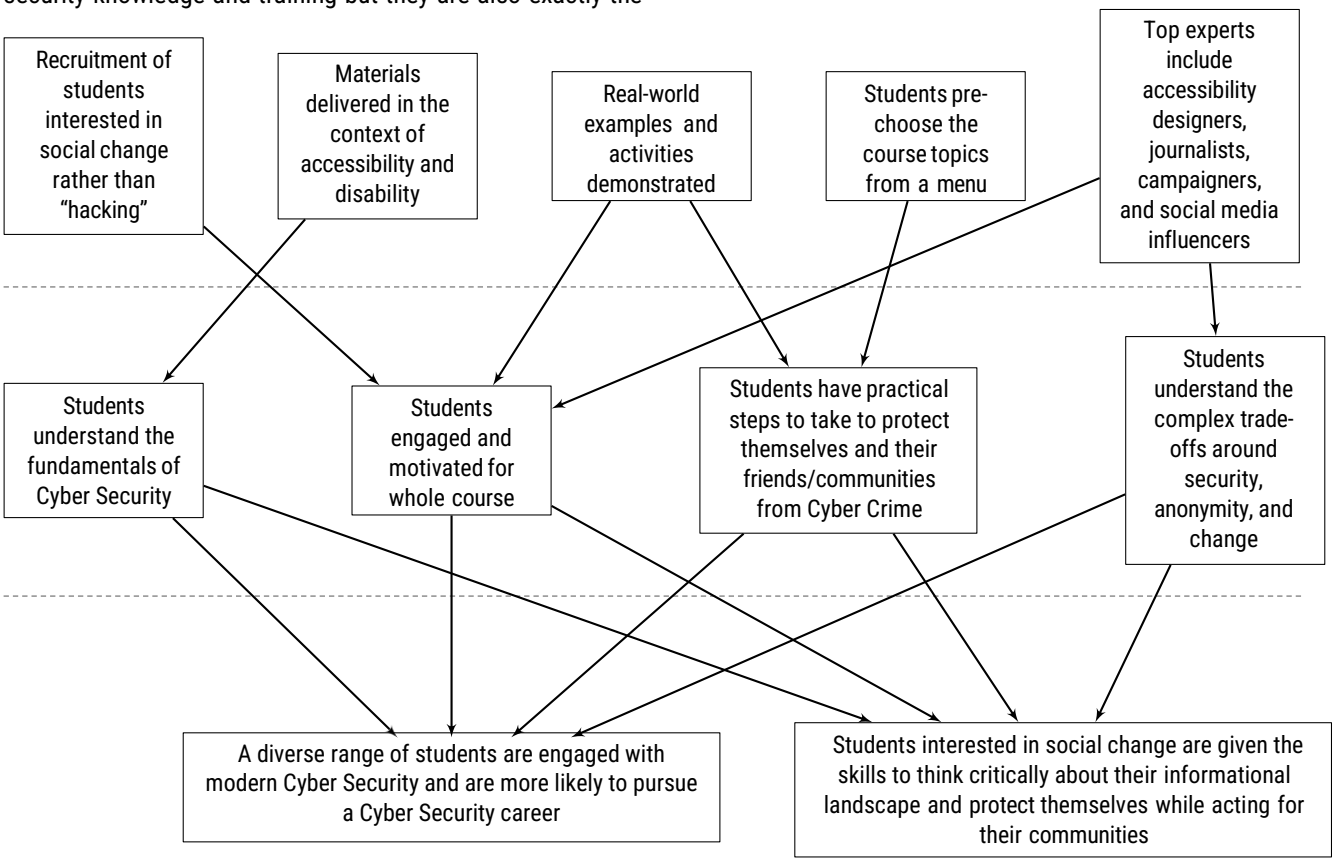

Fig. 2. The project's theory of change including activities (top row), outputs (middle row), and outcomes (bottom row).

The rest of this paper is organised as follows. Section II details how our newly proposed short course encourages the students to identify a social issue and reflect on the security implications of being involved in addressing that particular issue. In Section III we describe the course delivery and discuss its impact on developing the course resources. In particular, we test our material by delivering the course in two different schools in the UK, and produce a comprehensive guide to enable non-specialist teachers to use the material in a self-contained way. Finally, we share the received feedback and provide an outlook in Section IV.

II. COURSE DESIGN: STRUCTURE, LESSON PLANS AND CHALLENGES

We designed material for teachers to deliver a six lesson course on cyber security for digital activists, targeting as an audience young adults (16-18 year olds).[2]

From a student perspective, the structure of the course is as follows.

1. The students pick an aspect of change they would like to see in the world (anything from 'end climate change' to 'more cycle paths on the way to school').
2. The students are taken through six lessons on ways to affect change and on how to keep themselves safe in the process.

The lesson plans cover things such as management of information assets, risk assessment, and a wide range of case studies of activists dealing with numerous threats from bad actors. The vast majority of content is cyber security focused but contextualised into the world of social change.

A. Lesson Plans

We proposed six lesson plans that are designed to help students learn how to create social change in a safe and responsible way. The lessons cover a range of topics, and are structured to be flexible, allowing teachers to tailor the content to their students' needs and interests. For each lesson we developed slides, a teacher's guide and interactive activities. Illustrations and visual design of materials were provided by a professional artist (see Figure 4).

The six lesson plans are as follows.

- **Introduction** - In this lesson we start with a discussion and exercise on the topic of security in the broad sense - including motivations and capabilities of attackers. We then recast the social change aspect into more immediate and personal goals like "Start a fencing club" or "advocate against animal testing".
- **Information** - This lesson gives a framework for making changes and starts by asking the students to consider the difference between complaining and actually taking action to achieve change. The session focuses on information and includes an introduction to UK Freedom of Information requests.
- **Privacy and Threat Modelling** - This lesson examines a group of different activists and invites the students to understand why some conceal their identity and some don't. It examines a case study of a traumatic harassment campaign (we used Kiwi Farm's harassment of trans-rights activist Keffals [13]) and discusses the production of risk assessments.
- **Cryptography** - This lesson introduces cryptography and discusses how it is used to secure communications in general.
- **Complex Systems** - This lesson leads the students through a set of increasingly complex security systems – starting with the workplace, moving through friendships and relationships and ending with the family. For each example we discuss the challenges inherent to each context and how to manage them.
- **Scams, Magic, and Future Directions** - This lesson has three roles. It is a general overview of some common scam structures. It is also a chance to catch up on the progress of any projects started during the course, and finally it is something of a reveal - showing how the majority of the content of the course is from a cyber security background and what students can do to find out more.

While our lesson plans provide a comprehensive framework for teachers to follow, they are also designed to be flexible. If the whole group of students have a specific social change they are passionate about, teachers can focus on that topic and adapt the lesson plans as needed, allowing students to take ownership of their learning and work collaboratively to create meaningful change.

By nature, our lessons include some upsetting topics, and the students are asked to think quite carefully about the risks around issues that are important to them. We are clear in our materials that the potentially upsetting nature of the topics should be foregrounded and handled delicately. Our examples were chosen to illustrate issues without causing undue upset and the teacher pack contains alternate options.

B. On the use of Change Cards

One challenge we anticipated was that some students may be too afraid or shy[3] to express their ideas about social change. This can make it difficult to engage them in discussions and activities related to creating positive change. To address this, we created *Change Cards* (Figure 3) that contain a range of social issues, such as climate change, bullying, or poverty. These cards are randomly assigned to students during classroom activities, giving them a specific social issue to focus on during the exercise.

Fig. 3. The Change Cards we used on our course to help young people who might have been unwilling to share their particular hopes with the group.

The Change Cards serve several purposes. Firstly, they can help students who are too shy or scared to talk about social issues to overcome their fears and express their ideas in a safe and supportive environment. Secondly, the cards can help students focus their ideas and develop a plan of action for addressing a specific social issue. Thirdly, the cards provided 'plausible deniability' for students who wanted to ensure some separation between the change they wanted and their social identity in the school context. Finally, the cards can help teachers identify which social issues are important to their students, and tailor their lessons and activities accordingly.

C. *Our Theory of Change*

A Theory of Change (ToC) is a comprehensive framework, much used by the development community, that outlines how and why a desired change is expected to happen in a particular context [12], [14] (See [15] for a commentary on its use in STEM contexts).

We summarise our Theory of Change in Figure 2. Such diagrams are generally read from the bottom upwards: the final line is the 'outcomes' (the changes we wish to see from the project); the middle line is the outputs (the tangible/measurable changes caused by the activities), and the top line is the activities (things we are doing). Presented diagrammatically, it is easy to see if, for example, some activities are unnecessary, or some outcomes are being overlooked. We found having a diagrammatic Theory of Change extremely useful on the project for design, and for communicating our vision to funders and end-users.

III. COURSE DELIVERY AND DISCOVERIES

The initial materials were tested in two different locations in the UK: one Sixth Form College (i.e., pupils aged 16 to 18) on a weekly basis, and one set of secondary school students (i.e., pupils aged between 11 and 15) over a period of two weeks. Groups were between 15 and 20 students and attendance stayed reasonably strong through the course. Selection of groups was coordinated by teaching staff at the venues and attendance was voluntary. Feedback was collected by focus group and a limited number of surveys. Only qualitative feedback was acted upon; the group sizes were too small for quantitative feedback.

Some aspects of the content were changed after the testing, but in relatively minor ways; however the delivery experience was vital in terms of writing the lesson plans and guides for teachers that formed a key part of our resources.

After our testing, the whole resource pack was reviewed by an advisory board and a professional teacher before being launched online and made available on the project website for wide deployment and adoption. Dissemination was by Google Ads and targeted emails. Our focus was on creating a continuously growing body of work, where additional output from future runs of the course could be added to the project website.

A. *Unexpected Discoveries*

While we effectively targeted course materials for the desired students, we quickly discovered the need to treat school staff the same way. References to 'cyber,' 'digital', or 'online' led to our materials being directed to IT teachers and students, who were already well-versed in cybersecurity. To address this, we emphasised the social change aspects of the project in all school communication.

Our second unexpected discovery was that we had budgeted for journalists and other activists to speak to our test students following a model that was successful for [16]. The students couldn't have been less interested in the idea and we dropped it after the first couple of weeks. As per our theory of change in Figure 2, other activities were sufficient to achieve our outcomes.

B. *Expected Discoveries*

IT provision in UK schools (and 6th forms) remains (largely) effectively unusable. You cannot run an effective short intervention that involves students using a school computer. This was fine for us, but we would remind anyone designing a similar intervention that "you cannot assume there will be electricity".

Also, the students are genuinely keen to learn as long as the things are *real*. Small constructed examples don't really work for them, but examples of simple scams or crimes really do. Similarly "don't tell anyone your password" doesn't work but "at what point in a relationship would you give your partner access to your phone" produces exactly the sort of complex and nuanced discussion that the students need to have about security.

Professionalism is highly regarded in education. We commissioned an artist to illustrate and redesign our

resources (see Figure 4 for some examples) and the combination of strong visuals, solid fundamentals knowledge and student-centred context appears to be highly attractive to teaching staff. Finally, universities seem not to be set up for longer term dissemination of knowledge[4]: keeping domain names active, maintaining resources, promoting dissemination and keeping the project alive are all things that university bureaucracy is not set up for and it is vital to have an external project partner (as we did) that can handle both the promotion and legacy aspects of the project.

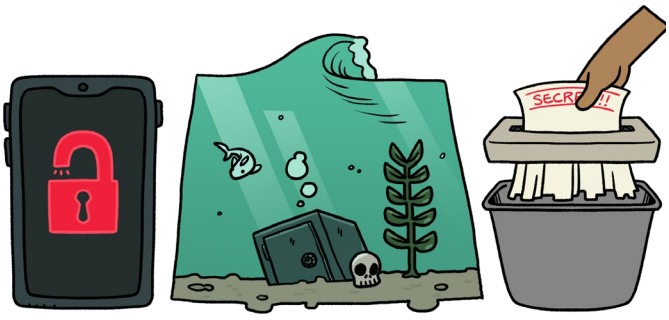

Fig. 4. We commissioned an artist who both drew illustrative examples on our resources and provided a general flair for design that makes our resources attractive to teaching staff.

IV. FEEDBACK AND OUTLOOK

To date, the lesson materials have been sought out and downloaded a little over 1,000 times by teachers wanting to deliver the course in their own classrooms.

The feedback has been excellent and we are excited that the work is already informing how young people deal with questions like, *Should I let my partner have the passcode for my phone?* or *I'm really passionate about this issue and want to campaign about it; how do I make sure I'm safe while I do*?

More specifically, students have said *I liked its relevance to day to day life,* and *How it improved my views of the concept of security"* and *I liked how we spoke about real world examples*.

Our guide for teachers has been very well-received. Some feedback was *The guide is well-written, well-presented and well-referenced. [...] The motivations and content are clear, varied and of good quality. The language is professional and still accessible. My colleague and I also agree that you have made a potentially intimidating topic area very easy to teach*.

Overall, the project successfully accomplished its goals of promoting cyber security education, expanding the understanding of cyber security beyond hacking, and empowering young adults to protect themselves and their communities in the digital landscape.

As practitioners, we are very aware that the field of cyber security in general is not as diverse as it could be [6], [7], and that the diversity issue applies not just to demographics but also to 'diversity of thought' and approach. It is our belief that finding a way to show these groups that cyber security can be relevant and interesting can only improve the diversity of the sector.

We believe the project's impact will continue to grow as additional content and feedback from future course runs are incorporated into the project website, making it a resilient tool in the landscape of cyber security education.

REFERENCES

[1] J. Nicholson, J. Terry, H. Beckett, and P. Kumar, "Understanding young people's experiences of cybersecurity," in *Proceedings of the 2021 European Symposium on Usable Security*, 2021, pp. 200–210.

[2] NSPCC, "Online grooming crimes have risen by more than 80% in four years," National Society for the Prevention of Cruelty to Children, Jul. 2022. Accessed: Sep. 9, 2024. [Online]. Available: Link no longer active.

[3] A. Sorrentino, F. Sulla, M. Santamato, M. di Furia, G. A. Toto, and L. Monacis, "Has the covid-19 pandemic affected cyberbullying and cybervictimization prevalence among children and adolescents? a systematic review," *International Journal of Environmental Research and Public Health*, vol. 20, no. 10, 2023. [Online]. Available: https://www.mdpi.com/1660-4601/20/10/5825

[4] B. Hassib and J. Shires, "Manipulating uncertainty: cybersecurity politics in egypt," *Journal of Cybersecurity*, vol. 7, no. 1, p. tyaa026, 02 2021. [Online]. Available: https://doi.org/10.1093/cybsec/tyaa026

[5] G. Coleman, *Hacker, hoaxer, whistleblower, spy: The many faces of Anonymous*. Verso books, 2015.

[6] X. Mountrouidou, D. Vosen, C. Kari, M. Q. Azhar, S. Bhatia, G. Gagne, J. Maguire, L. Tudor, and T. T. Yuen, "Securing the human: A review of literature on broadening diversity in cybersecurity education," in *Proceedings of the Working Group Reports on Innovation and Technology in Computer Science Education*, ser. ITiCSE-WGR '19. New York, NY, USA: Association for Computing Machinery, 2019, p. 157–176. [Online]. Available: https://doi.org/10.1145/3344429.3372507

[7] M. Namukasa, C. Ficke, I. Piasecki *et al*., "Understanding how to diversify the cybersecurity workforce: A qualitative analysis," *Journal of Cybersecurity Education, Research and Practice*, vol. 2023, no. 2, p. 4, 2023.

[8] J. Blasco and E. A. Quaglia, "InfoSec cinema: Using films for information security teaching," in 2018 *USENIX Workshop on Advances in Security Education (ASE 18)*. Baltimore, MD: USENIX Association, Aug. 2018. [Online]. Available: https://www.usenix.org/conference/ase18/presentation/blasco

[9] R. Sandoval-Almazan and J. R. Gil-Garcia, "Towards cyberactivism 2.0? understanding the use of social media and other information technologies for political activism and social movements," *Government information quarterly*, vol. 31, no. 3, pp. 365–378, 2014.

[10] ChatGPT, "Image of a cyber security professional," Generated using ChatGPT, 2023, image generated by ChatGPT in response to the prompt: "What does a cyber security professional look like?". [Online]. Available: https://chat.openai.com/

[11] Midjourney, "Image of a cyber security professional working at a desk," Generated using Midjourney, 2023, image generated by Midjourney in response to the prompt: "a cybersecurity professional working at a desk". [Online]. Available: https://www.midjourney.com/

[12] S. C. Funnell and P. J. Rogers, *Purposeful program theory: Effective use of theories of change and logic models*. John Wiley & Sons, 2011, vol. 31.

[13] N. Tiku, "The endless battle to banish the world's most notorious stalker website." *The Washington Post*, pp. NA–NA, 2023.

[14] P. Barbrook-Johnson and A. S. Penn, "Theory of change diagrams," in *Systems Mapping: How to build and use causal models of systems*. Springer, 2022, pp. 33–46.

[15] D. L. Reinholz and T. C. Andrews, "Change theory and theory of change: what's the difference anyway?" *International Journal of STEM Education*, vol. 7, pp. 1–12, 2020.

[16] Y. Skipper, D. Jolley, and J. Reddington, "'but wait, that isn't real': A proof-of-concept study evaluating 'project real', a co-created intervention that helps young people to spot fake news online," *British Journal of Developmental Psychology*, vol. 41, no. 4, pp. 371–384, 2023.

NOTES

1. In general, we can say that cyber security has an ongoing problem with diversity, particularly as a result of this ongoing disconnect [6], [7].
2. Six lessons is a common length for 'personal, social, health and economic' topics in the UK.
3. Or, at the start of the lessons, disengaged.
4. This is a shocking sentence to write and we don't do so lightly.