

# Understanding Young People's Experiences of Cybersecurity

James Nicholson

Northumbria University, Newcastle, UK, james.nicholson@northumbria.ac.uk

Julia Terry, Helen Beckett, Pardeep Kumar

Swansea University, j.terry@swansea.ac.uk, helen.beckett@swansea.ac.uk, pardeep.kumar@swansea.ac.uk

Young people are increasingly becoming responsible for the security of their devices, yet do not appear to have the knowledge to protect themselves online. In this paper, we explore young people's knowledge of cybersecurity through a series of workshops with secondary school children, and co-design cybersecurity lessons aimed at engaging this demographic. We find that technical demonstrations are an effective way of engaging young people's curiosity in the subject, and that group activities aimed at exploring the subject are preferred methods. We also find that while knowledgeable about cybersecurity theory (e.g. passwords), their actual behaviours did not reflect best practice. We discuss the role of schools in cybersecurity education and how to best embed this content in the curriculum to maximise the engagement of students, including a focus on teaching about cybersecurity protective tools.

CCS CONCEPTS • Security and privacy ~ Human and societal aspects of security and privacy ~ Social aspects of security and privacy.

**Additional Keywords and Phrases:** Children, cybersecurity, digital citizenship curriculum.

## ACM Reference Format:

First Author's Name, Initials, and Last Name, Second Author's Name, Initials, and Last Name, and Third Author's Name, Initials, and Last Name. 2018. The Title of the Paper: ACM Conference Proceedings Manuscript Submission Template: This is the subtitle of the paper, this document both explains and embodies the submission format for authors using Word. In Woodstock '18: ACM Symposium on Neural Gaze Detection, June 03–05, 2018, Woodstock, NY. ACM, New York, NY, USA, 10 pages. NOTE: This block will be automatically generated when manuscripts are processed after acceptance.

## 1 INTRODUCTION

With the advancement and ubiquity of technology, children in the Western world are being exposed to smartphones, tablets, and gaming systems from as early as 1 year old, and by age 4 many children already own a mobile device [13]. Increased exposure to the internet has highlighted the need for security education to be directed to young age groups, especially considering the rise in cases of identity fraud amongst children in the US which superseded 1 million cases and \$2.6 million in total losses in 2017 [31]. However, formal computing education is primarily geared towards personal safety (or *e-safety*) highlighting the issues of cyber predators using social media and games, sexting, searching and cyberbullying. Meanwhile, formal education

for secondary school children about maintaining the digital security of accounts and devices (e.g., password management) is given far less priority and children are expected to protect their accounts and devices with less explicit cybersecurity knowledge [30].

While e-safety is of utmost importance for children, a more rounded cybersecurity education should be a growing priority as children are more frequently accessing their own devices and accounts on various services without adult supervision [13]. Even when adult supervision and guidance is provided, we know that many adults do not understand or follow cybersecurity best practices [25] which can result in passing on flawed practices.

Through the Digital Citizenship Curriculum (DCC) – a set of lessons that aim to teach children about how to use technology responsibly – we are starting to see schools address young people’s lack of security knowledge in a more systematic way. Aspects of Digital Citizenship include both cybersecurity topics, including password management and scam detection, along with other more safety-oriented topics like cyberbullying and privacy [22]. However, there are suggestions that these approaches have not been as successful as hoped [23] and we continue to see this with research highlighting children’s poor password practices [21] and poor phishing detection [26]. With this in mind, we set out to capture a better understanding of children’s experiences around cybersecurity and how we might engage them with the topic.

In this paper, we take a first step towards answering the following research questions:

- RQ1: What general online security concepts are young people aware of?
- RQ2: How are young people learning about these online security concepts?
- RQ3: What are young people's preferences for learning cybersecurity concepts?

Our key contribution is the co-design of a formal cybersecurity session with school children with the purpose of understanding what aspects of the topic they find interesting and enjoy, while also exploring what activities are desirable for ensuring engagement with the learning process. As far as we are aware, the design of cybersecurity learning sessions has not been previously explored in an early secondary school context.

## **2 RELATED WORK**

Over the past few years, researchers have started paying attention to digital risks for children and pushing cybersecurity education. Existing studies in this domain have predominantly explored children’s password management strategies and insights into their knowledge around phishing detection.

Children use technology and online services that require frequent authentication. However, currently there is sparse research on how children authenticate and protect themselves online. Choong et al. [8] surveyed password knowledge and practices of children aged 8-15 years, observing that children showed confusion between the concepts of passwords, privacy and safety or protection. Age was found to be a factor in password practices, with the younger children relying on parents for creating and remembering passwords while older children created longer passwords compared to younger children. Maqsood et al. [21] studied how children aged 11-13 years created passwords given different password policies. They observed that children created simple passwords containing their personal information such as name or age and believe that their passwords

would be hard for a stranger to guess, and generally showed poor understanding of how passwords should be created. Similarly, other researchers have observed that children create passwords containing whole words and personal information and have trouble recalling long and complex passwords compared to simple ones [19]. Other work [9] has observed that 6-12 year olds are not necessarily better with graphical passwords – alternatives to passwords which have traditionally been considered easier to use for certain populations [24]. In fact, surprisingly, their study on 13 participants showed that the success rate for the click-based graphical password was lower than that for alphanumeric passwords. These studies collectively demonstrate that both younger and older children demonstrate poor cybersecurity hygiene and suggest that there may be issues with how this information is being taught to this age group. However, more recent work looking at how children manage their passwords has found that they are beginning to understand the importance of security mechanisms like passwords, but their implementation of these still leaves a lot to be desired [7].

Young people's poor awareness of cybersecurity of course extends beyond passwords. Lastdrager et al. [20] investigated the effectiveness of anti-phishing training for school children aged 9-12 years and found that their poor phish detection performance could be improved through age-appropriate training, yet only temporarily. Similarly, more recent work has also demonstrated how teenagers perform poorly in phish detection tasks [26], again highlighting important issues in security awareness and behaviours amongst young users.

While historically we have seen guardians take the responsibility for ensuring that children remain safe online [18], this is problematic given the well-documented issues that adults have around cybersecurity mental models [11,25,37] which can then be passed on to younger people. Recently, Western schools have begun to implement a DCC that aims to empower children and young people via education and/or via their active and responsible participations in the digital societies and technologies [17]. The aim of the DCC is to cover relevant areas of digital technologies and interactions to ensure that children's skills are appropriate, but also to ensure that they can safely manage the digital world. This content is expected to cover data security aspects, such as password management and scam detection, but in practice it generally appears to focus on privacy and cyberbullying (i.e., e-safety) [12]. This is supported by other work focusing on the insights from the educators [22], but this may be in part due to educators not always having the necessary advanced levels of digital citizenship which may then translate to gaps of knowledge for students [6]. Of course, this then means that poor cybersecurity behaviours, such as the usage of weak passwords, continue amongst this population [23].

### **3 METHOD**

Our study set out to establish young people's existing knowledge and current cybersecurity education experiences, and to explore how young people wished to learn about cybersecurity in the future. By understanding the preferences of young people through exploration and engagement, good practice can be established on how best to educate young people in protecting themselves from cyberattacks. Opportunity was sought to engage with young people to not only establish what knowledge they already held, but to raise awareness of cybersecurity and healthy digital habits. In order to do this, we held two full-day university-based workshops with three secondary schools where young people attending could learn more about risks and consequences of poor cybersecurity habits and about positively engaging online (see Figure 1). We ran one mixed workshop with two schools and another workshop with one school, where young people were encouraged to engage in pre- and post-workshop questionnaires about their cybersecurity knowledge, and to discuss related topics in focus groups.

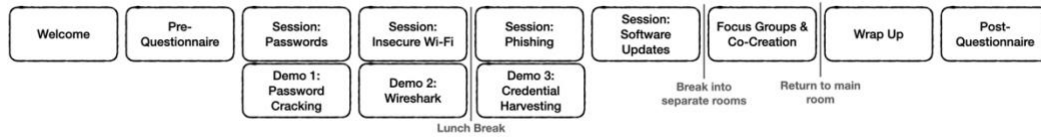


Figure 1: Timeline of activities for each full-day workshop.

The aim was to work in partnership with young people in creating engaging solutions to meet their cybersecurity education needs. A mixed methods approach was used, combining quantitative (the questionnaires) and qualitative (the workshops) approaches to achieve a greater understanding of young people’s cybersecurity habits.

### 3.1 Participants

We recruited 50 young people aged 12-14 years old from three different secondary schools (25, 10, and 15) to participate in university workshops via a university outreach program. We specifically targeted schools that ranked in the lower quartile of underprivileged schools in the area to ensure a realistic representation of the DCC. An email advert about the workshop opportunity was sent to schools from our partner instructing them to contact the university to register interest. Once workshop places were filled, information about this specific research opportunity were sent with participant information sheets for young people, and their parents/guardians, as well as consent forms for parents/guardians to complete beforehand (see 3.4 for more details). Due to data protection and ethical guidelines we are unable to report on more participant details including mean age, or specific demographics, which is a limitation of this study.

### 3.2 Demonstrations and Cybersecurity Topical Content

The informational content of the workshop was based on the UK’s National Cyber Security Centre’s citizen advice on staying safe online<sup>1</sup> and focused on the key password management, scam detection, and software updating behaviours – matching the content on the pre- and post-questionnaire. The format used for each topic consisted of presenting the basics of the security problem (information session), followed by a live technical demonstration of this attack, then we discussed prevention techniques and tools, and finally answered questions. The demonstrations were sandboxed, meaning that participants’ user accounts and/or devices were not targeted in the process, only accounts and devices that were set up prior to the demonstration sessions. This was the case for 3 of the topics, with software updates not including a demonstration due to time constraints and lack of unique demonstration content.

**Demonstration 1: Password Cracking Using John the Ripper.** The first demonstration showcased the ease with which weak passwords can be guessed using an open-source computer program (John the Ripper, see Figure 2) and a password file obtained from a well-known data breach.

<sup>1</sup> <https://www.ncsc.gov.uk/cyberaware/home>

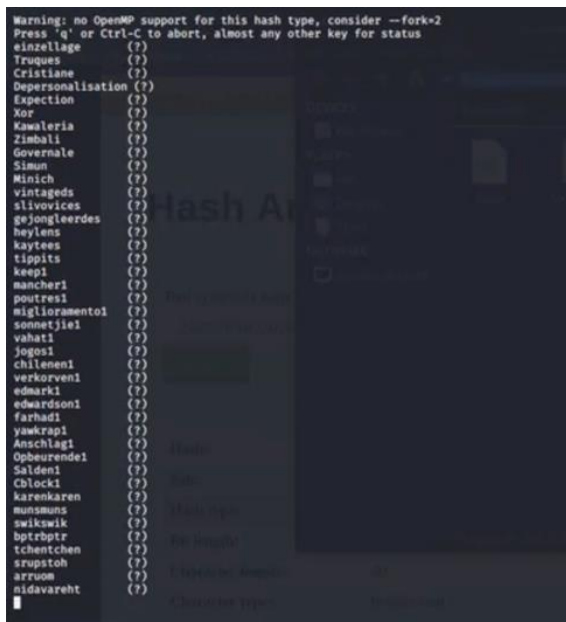


Figure 2: Password guessing using John the Ripper in action.

Participants were shown how a large list of password hashes could be guessed in a few minutes using two dictionaries (*all.lst* and *rockyou.txt*) and a brute force attack.

**Demonstration 2: Packet Capture using Wireshark.** The second demonstration showcased how data packets transferred using an unsecured Wi-Fi network can be captured and viewed (see Figure 3) using the Wireshark open-source software.

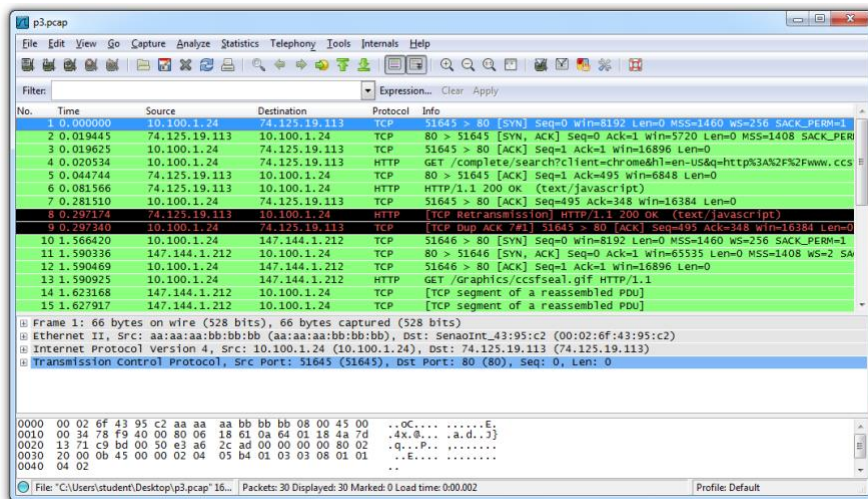
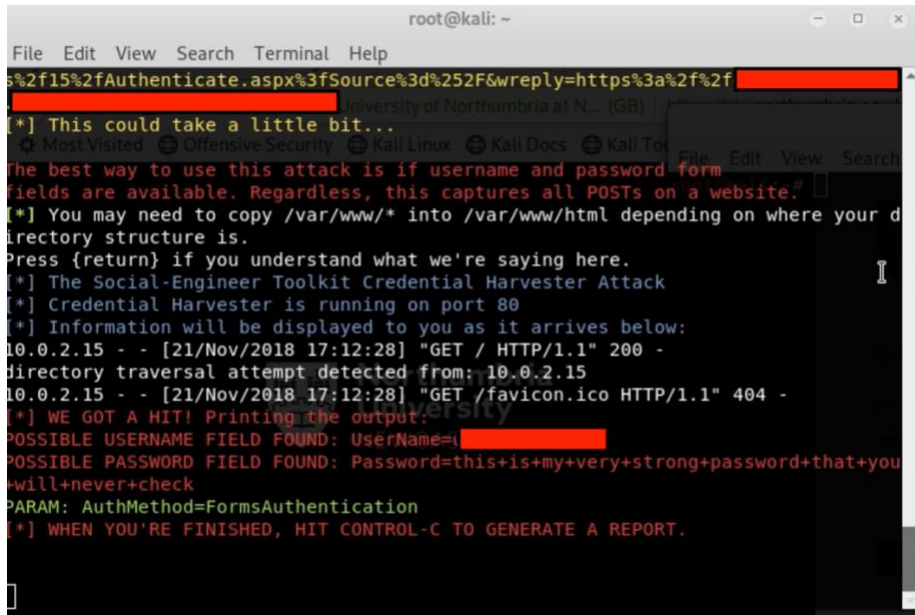


Figure 3: Using Wireshark for data packet capture.

**Demonstration 3: Creating a Credential Harvesting Phishing Website.** The final demonstration showcased how the open-source software package, the Social Engineering Toolkit, could be used to clone a social media website (Facebook) and harvest credentials of unsuspecting users (see Figure 4).



```
root@kali: ~
File Edit View Search Terminal Help
5%2f15%2fAuthenticate.aspx%3fSource%3d%252F&wreply=https%3a%2f%2f
[*] This could take a little bit...
The best way to use this attack is if username and password form
fields are available. Regardless, this captures all POSTs on a website.
[*] You may need to copy /var/www/* into /var/www/html depending on where your d
irectory structure is.
Press {return} if you understand what we're saying here.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
10.0.2.15 - - [21/Nov/2018 17:12:28] "GET / HTTP/1.1" 200 -
Directory traversal attempt detected from: 10.0.2.15
10.0.2.15 - - [21/Nov/2018 17:12:28] "GET /favicon.ico HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: UserName=[REDACTED]
POSSIBLE PASSWORD FIELD FOUND: Password=this+is+my+very+strong+password+that+you
+will+never+check
PARAM: AuthMethod=FormsAuthentication
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

Figure 4: Credential harvesting website in action (some text removed for anonymity).

The demonstration included the cloning of the website as well as showcasing the capture of user credentials.

### 3.3 Procedure

We collected our data through two university-based workshops (see Figure 1 for structure of activities) with three local schools participating in total. Questionnaires were used to capture young people's knowledge of key cybersecurity topics before and after the workshops (see Table 1 for questions). The pre- and post-workshop questionnaires were identical and consisted of open-ended questions where the young participants could expand on their answers.

The workshops began with an introduction and icebreaker activities, and further information about the research project. All young people were invited to participate in pre- and post-workshop questionnaires and focus group discussions, which they had been informed about before attending but it was made clear that there was no onus on them to participate, and that alternative activities were available if they did not want to take part. Young people were then invited to complete consent forms (see 3.4 for more details). During the workshops, young people engaged with cybersecurity activities and demonstrations, and all attendees chose to participate in the research activities. The technical demonstrations were performed live and consisted of guessing passwords from a well-known data breach using a password cracker, intercepting authentication credentials through insecure Wi-Fi, and the creation of a cloned phishing website (see 3.2 above and Figure 1).

Five focus groups were undertaken across the two workshops, with each group facilitated by two members of the research team, and each group accompanied by one of their teachers. Focus groups began with facilitators reading out ground rules, and then a quick ice-breaker activity where participants were encouraged to discuss their use of social media. The questions then moved towards cybersecurity, with prompt questions including how important the topic of cybersecurity was to them or not, what young people think about cybersecurity, and their understanding about being hacked. Finally, we ran an activity with each focus group where children were supported to co-design their ideal cybersecurity lesson for a school, consisting of group time to draw and shape their lesson followed by a 'show and tell' to the group. All focus groups were digitally recorded and transcribed verbatim. Each workshop session lasted 5 hours.

### **3.4 Ethics**

Ethical approval was obtained at the outset from the University's Research Ethics committee. As all potential participants were under 18 years of age, information sheets were sent out to all parents/guardians and young people (through schools) to raise awareness of the proposed study, with an opportunity to engage with the research team for further information, and a clear message that there was no onus on young people to take part. Parents/guardians were given two weeks to withdraw their children from the workshop. All young people who participated at university workshops were informed that they could engage in the workshops without participating in all or part of the research elements. A teacher from each school was present throughout, and engaged in all aspects of the workshops, providing a known face to the participants if they had queries.

Following completion of the pre-workshop questionnaires, young people spent time engaged in information and demonstration sessions to allow opportunities to increase their understanding about cybersecurity in the future. At the close of each workshop attendees were provided with a small goodie bag with pens, USB flash drive and a cybersecurity infographic as take-home information.

### **3.5 Analysis**

#### *3.5.1 Quantitative*

We developed a simple questionnaire to test young people's knowledge of key cybersecurity knowledge (as defined by the UK's National Cyber Security Centre) including 11 questions around the definitions and examples of password management, phishing, two factor authentication, software updates, Wi-Fi security, and steps to remedy a hacked account (see Table 1 for the wording of a subset of questions). The questionnaire was filled out by participants upon arrival before starting the content delivery and activities. A second identical questionnaire was then filled out at the end of the day prior to the conclusion of the workshop.

The individual questions for each respondent were scored as either correct or incorrect based on academic and professional best practice. Data was then analysed using a paired samples t-test between the pre-workshop and post-workshop scores.

#### *3.5.2 Qualitative*

The five-person research team (which included individuals from nursing, computer science and law), were involved in all aspects of analysis to minimise potential bias and/or preconceptions of any individual researcher. Researchers began by reading focus group transcripts and applying a thematic analysis approach [5], both

independently (to produce a tentative thematic framework), and then together for cross collaboration and discussion, to identify and agree recurring themes.

#### 4 FINDINGS

First, we looked at how the presentation of cybersecurity content in a workshop setting, including demonstrations and discussions, affected the knowledge of young people. We found a statistically significant difference between the scores of pupils before the workshops (53%) and their scores after the workshop (88%),  $t(49) = 8.273, p < .001$ . This clearly demonstrates that the pupils improved their knowledge of key cybersecurity behaviours while taking part in the workshops. While it is generally to be expected that participants will immediately improve their performance following a knowledge session, it was important to establish that the methods we chose to convey this information to this group was at least not detrimental.

The most problematic knowledge areas (i.e., lowest scoring) prior to the workshops consisted of phishing messages (29% right responses), knowledge of password managers (38%), knowledge of two-factor authentication (38%), and knowledge of software updates (41%) (see Table 1). Overall knowledge about password composition (95%) and not reusing passwords (81%) was very good, with nearly all pupils being aware of best practice guidelines.

*Table 1: Cybersecurity knowledge prior to the workshop (from questionnaires).*

Questionnaire Item	Successful Response Rate (n = 50)
What is “phishing”? Please provide one example.	29%
If you suspect a message is phishing, name two things you can do to check if it is or not.	33%
What helps make a “strong” password? Please provide one example	95%
Why should you not re-use passwords on multiple accounts?	81%
Name two benefits of using a password manager.	38%
What is “two-factor authentication” (also known as 2FA)? Please provide one example.	38%
What are software updates? Why are they relevant to cybersecurity?	41%
What can happen if you use public Wi-Fi for sensitive activities?	71%

Following the workshop, when completing the same questionnaire all cybersecurity knowledge areas improved, although the importance of software updates and their relevance to cybersecurity remained as the worst performing item (55%), with nearly half of all respondents not understanding how the security of a system could be improved through software updates.



Table 2: Cybersecurity knowledge after the workshop (from questionnaire).

Questionnaire Item	Successful Response Rate (n=50)
What is “phishing”? Please provide one example.	100%
If you suspect a message is phishing, name two things you can do to check if it is or not.	100%
What helps make a “strong” password? Please provide one example	100%
Why should you not re-use passwords on multiple accounts?	100%
Name two benefits of using a password manager.	83%
What is “two-factor authentication” (also known as 2FA)? Please provide one example.	86%
What are software updates? Why are they relevant to cybersecurity?	55%
What can happen if you use public Wi-Fi for sensitive activities?	83%

Below we report on our qualitative findings predominantly based on the five focus groups held with the pupils following the initial workshop demonstrations. Some insights are drawn from other interactions during the full-day workshop, but all quotes are from the formal focus group sessions. For privacy reasons we attribute each quote to a focus group, rather than an individual pupil (e.g., Focus Group A-E)

#### 4.1 Knowledge and Behaviours

Supporting our questionnaire findings, all five focus groups demonstrated that young people had a good understanding of cybersecurity threats, and that their mental models matched to a large extent the landscape of threats to their personal information.

*“I think it’s quite dangerous because they collect your personal information especially on social media and stuff, because you have put in some personal information to go on there, so they can hack into your personal data and information and stuff”* (Focus Group A)

This at first appears to be normal – these young people are perceived as being *digital natives* [1] who have grown up with the internet and thus are expected to understand the mechanics and pitfalls of this technology. Specifically, as reported in our questionnaire findings above, our young participants exhibited good conceptual knowledge of several important aspects of cybersecurity. In particular, they demonstrated excellent awareness around password management.

*“You can best protect yourself by, like, having passwords that’s long enough but also complicated enough so like hackers can’t get into it as easily”* (Focus Group C)

Their understanding of what makes a strong password, the importance of unique passwords, and the necessary steps required once discovering an account breach was surprisingly accurate across participants and across focus groups. This is particularly surprising given previous work suggesting that this age group have a poor understanding of password composition and management [8,19,21], but does support more recent work

[7] as well as being in line with research looking at children's understanding of privacy risks [40]. However, as foreshadowed by our quantitative findings, their knowledge and understanding of tools that could support these behaviours was lacking. Even when participants had been motivated to use these tools, they quickly became demotivated and ceased to engage with them.

*"I've used [2 Factor Authentication]... but it just takes more of my time... I use it sometimes for some of my accounts, like Instagram and stuff"* (Focus Group D)

The young participant above recounts how they enabled two-factor authentication on their accounts to "be more safe" after being encouraged by a friend, but soon disabled it for their most used accounts due to the time taken to log in. However, this extra layer of protection remained active on accounts that they accessed less frequently. This relates to prior work demonstrating that users have a tendency to abandon privacy and security tools when they find them inconvenient [41] yet here we see how this can also be common in a younger population despite having first-hand experience of having their online security compromised (see below). Although young people showed good knowledge of cybersecurity, this did not necessarily mean that it was translated into good cybersecurity habits.

*"Well, I just haven't really found the need for [a password manager]. I don't have too many different passwords. I don't really use too many things"* (Focus Group B)

Citizens making decisions based on convenience rather than security is not new or surprising [38]. However, in this case it is particularly striking due to our participants' very clear understanding of the security threats associated with that convenient choice. A possible factor, as highlighted by the participant above, could be that in their limited experience they have only had to manage a handful of codes as opposed to adults who typically manage an average of 26 *regular* codes [32], and thus may believe that the problem is overblown. However, the expectations of this age group may also factor into their decisions to ignore security advice.

*"If I am honest, I think there is so much information shared across these that are owned by organisations anyway, that I don't think people really care that much about how much it is hacked"* (Focus Group D)

The participant above explains how both account hacking and online tracking have been normalised for this age group, with other participants agreeing that they "have almost come to accept the fact that I am likely to be hacked" (Focus Group B). There were numerous examples from participants of friends' accounts being hacked (e.g., Fortnite), a large number of email and SMS scams that were successfully identified both by the participants and their friends, as well as regular interactions with gaming bots looking to scam them. Many of our participants also had first-hand experiences of being successfully compromised (ranging from account takeovers to installing malware), yet despite these experiences many had not improved their own security (i.e. they set up a new account with same password), suggesting that established triggers for behaviour change in adults may not necessarily apply to younger people [10].

## 4.2 Existing Learning and Support Structures

Our young participants reported learning about specific hacks and potential prevention techniques from a range of social actors, but in particular friends and siblings. As documented previously, friends play a key role in sharing methods for staying safe online (e.g. 2FA), even if these social interactions then do not lead to long-term change. Siblings were reported as influential, both in facilitating bad practice (accessing social media platforms earlier than the required age) as well as being supportive about password information.

*“One time my Roblox account got hacked so my sister changed the password to the new password”* (Focus Group C)

Young people also reported that they could learn from siblings’ mistakes, like getting hacked. These teachable moments can provide good opportunities for friends and family to offer advice, and young people recognised the value of having information disclosures before bad things happen.

*“Because I know my sister had a TikTok account and then one time she forgot to put her account private and, like, you were saying that random people were liking individuals, so my dad had to... take her phone, delete everything, remove all her password and everything, literally delete the whole account and then she got it back and she set it up private and only people from her class could see it and then she doesn’t really use it much now...”* (Focus Group A).

The family environment clearly has an important role to play in creating awareness around security and privacy issues, as prior work has identified the importance of security stories for awareness and behaviour change, with informal stories from friends and family being the most common method [33]. However, despite seeing the value of these open sharing opportunities, many acknowledged that these were typically limited in formal school settings (see 4.3), but also in particular at home.

*“In school we have assemblies or meetings about it, and how we can stay safer. But at home, like I won’t really talk about it, because it is not a big subject in my mind.”* (Focus Group D)

In fact, participants commented that their own support networks were mixed, which resonates with prior literature reporting that security and privacy topics are not openly discussed in a home environment [39]. Despite the lack of open discussions, participants suggested that parents could be available for emotional support if they had concerns about the internet and being hacked, in line with previous work demonstrating that guardians are the main support network for children, but this usually happens in a passive rather than active way [18]. Participants also reported that they did not feel listened to when they talked about the technicalities of cybersecurity at home, despite often sharing what they had learned on the topic at school.

*Young Participant1: “I think parents should listen more to their children but they don’t because we could be talking about something really important and they wouldn’t listen and they won’t know about it.”*

*Young Participant 2: “Sometimes I’ll tell my parents something and my mum will have to search it up because she doesn’t believe me.” (Focus Group B)*

This matches previous work showing that privacy and security are not typically discussed openly in families [39], but here we see how this can be particularly problematic for young people and in fact may put them off completely discussing these matters with parents. Interestingly, participants also reported that they had learned about cybersecurity and how to protect themselves online from web adverts.

*“Sponsorship, on videos, like when they’re being sponsored, talking about password managers and...I was watching a video, I can’t remember the name of the company but, you know, it was sponsorship for this password manager thing, what they’d recommend for a strong password and how it works and stuff” (Focus Group E)*

This unexpected source of information suggests that these pop-up messages could influence and improve young people’s online behaviours, and as such should be explored in more detail to better understand how these might be used to supplement more formal sources of cybersecurity information.

### **4.3 Engaging with Cybersecurity Learning**

As was mentioned in the previous subsection, young people learned about cybersecurity through social means including discussions with friends, siblings, and to an extent parents. However, when exploring formal learning methods, it was clear that many of our participants had experiences of learning about cybersecurity from schools in a piecemeal approach. For example, it was very common for participants to report first learning password composition in primary school, followed by how to safely use social media (e.g., information disclosure), and eventually progressing to social engineering such as phishing later on at secondary school. This scaffolded method was at large appreciated by our young participants, although the majority suggested a more ingrained and consistent approach to learning this type of content, rather than relying on “*special lessons*” and events like Internet Safety Day. Instead, little and often was seen as a more fruitful approach.

*“So I think we should have, like, a little [session] every Friday morning or something so it sticks in your mind” (Focus Group C).*

A large part of the focus groups with our participants focused on understanding key aspects of their engagement with the topic, in part based on their experiences at school, outside school, and during the earlier part of the workshop session. Here we report on key recurring aspects that were discussed by our participants across the five focus groups: demonstrations, group activities, games, and extended support.

#### **4.3.1 Live Demonstrations and Videos**

Our young participants expressed great curiosity around the security attacks throughout the workshop, illustrated by their regular questioning of the research team. After the demonstration of the cybersecurity attacks, even more questions were asked by our participants. In fact, our young participants reported that the

demonstration of these attacks were helpful for better understanding what the problem was and how they might protect themselves in the future.

*“Because you probably think, like I thought, people would just guess my password, I didn’t think about computer programs searching and having the ability to do that”* (Focus Group A).

The construct of curiosity is known to be an important motivational aspect for encouraging learning in children [15]. Curiosity has been explored in the context of privacy comprehension and disclosure [16], but not much work has focused on engagement for learning about security specifically. However, from what we can see here, it may be possible to draw pupils in with tailored demonstrations which will open discussions around the topic. Importantly, viewing these demonstrations also raised questions on *why* someone would conduct a cybersecurity attack (e.g. credential stuffing attack, or a phishing attack) as well as *what happens after* this attack. The majority of follow up questions focused on these two aspects, and directs us to towards exploring the possibility of crafting demonstrations not only showcasing how the attacks happen, but perhaps covering the stages before and after the attacks for full engagement and understanding. Demonstrations have been reported as being particularly useful when training adults on cybersecurity topics [27], yet this work has predominantly focused on older adults rather than young people. It is well known that children can learn motor skills [35] and behaviours [29] through modelling (a form of demonstrations), and that demonstrations for advanced concepts in other disciplines can help significantly improve understanding [4]. Similarly, tutorials – consisting of PowerPoint slides and narration – have been used in a security context to help adults improve their mental models of cybersecurity protocols [3], as have interactive stories [34], but these perhaps relate better to pre-recorded videos: In addition to live demonstrations, our participants were very keen for videos depicting *“everyday life examples”* that followed a similar format to live demonstrations.

*“So, I saw a documentary on public Wi-Fi, and there was two people sitting in a room, and one of them was in a bar, and they were sitting at the bar and they logged into public Wi-Fi, and it wasn’t the actual domain, it was going through somebody else’s laptop, and that laptop then created a connection to boost its signal off the Wi-Fi and then they took everyone’s payment details and everything through that. So, actually they created like a Wi-Fi log in screen that made it look like it was the actual Wi-Fi, and it wasn’t.”* (Focus Group B).

This participant goes on to explain how viewing this video has made them more cautious of using free Wi-Fi, and resonates with similar comments following the live demonstration. In an ideal world, any session focusing on cybersecurity would have *“quite a few videos in there”* (Focus Group C). Previous literature has begun to look at how videos can be designed appropriately to improve the adoption of cybersecurity tools [2], but more work is needed to understand whether these design decisions are also applicable to a younger population and whether story-driven or technical videos are more effective.

#### 4.3.2 Group Activities and Support

Participants agreed that in addition to more passive demonstrations of attacks (live or recorded), more practical activities, similar to those depicted in the demonstrations, would help them better engage with learning this topic.

*“Also have activities for the children. So, like, say, we were learning about hacking, you’d maybe give them a computer just to trial out, but obviously, make sure it’s not real accounts... So, like, giving them certain tasks to do, like, putting certain things together, trying to figure out passwords and that”* (Focus Group C).

A caveat here, according to a number of participants, was that the group activities should involve friends and not young people they did not already know, as this would make the environment less conducive to learning. This condition is not unprecedented in the education literature: Social affinity between children has been found to be important for motivating children to learn in collaborative settings, and this includes friendship between partners [36]. From a security perspective, we have seen how adults are able to form their own support groups when learning new cybersecurity topics [28], but more work is needed to understand these types of dynamics with a younger population in this context.

#### 4.3.3 Formal Peer Support

In addition to having hand-on experience with cybersecurity, participants from a specific school described an initiative that allowed some students to learn more about technology and security in order to then help other students in their school. This initiative, called the Digital Leaders, consisted of the IT team selecting a few older students and teaching them more in-depth content so they can then support other students in the school through videos, in assembly, and generally while at the school premises. This was a particularly good initiative as the pupils could *“relate to it”* (Focus Group D) and suggests that other schools may benefit from similar approaches. In fact, recent work has explored peer-to-peer cybersecurity in older adult communities with positive findings [28], so rolling this within schools may be a step in the right direction.

## 5 DISCUSSION

This paper has reported on two full-day workshop sessions with 50 school children aged 12-14 where we explored their existing knowledge of cybersecurity topics and co-designed a cybersecurity lesson. Below we summarise our key findings and discuss important insights from our work.

### 5.1 RQ1: What general online security concepts are young people aware of?

Young people, based on our sample, were very knowledgeable about some security topics: In particular, their mental models around password management were excellent. This was surprising given previous work showing that young people’s understanding of password composition is poor [21] but also starts to resemble more recent work around accurate mental models [7]. Despite their good conceptual knowledge, in practice their password management behaviours resembled those of the general population [32]. Other cybersecurity knowledge and behaviours, for example phishing, were poor, supporting previous work in this area [26]. We can extend this work now through insights on how cybersecurity is currently taught at schools, with social engineering (including phishing) typically being covered later on in the curriculum. We also noted a worrying trend of desensitisation to hacking, where many young people believed they would be hacked at one point and therefore failed to see the need for extra security.

## **5.2 RQ2: How are young people learning about these cybersecurity concepts?**

Young people learn about cybersecurity concepts both informally and formally. Informally, young people appeared to learn about cybersecurity concepts through social interactions with friends and siblings predominantly, as well as through online advertising (e.g., on YouTube videos). While parents were a trusted point of call for fixing issues or handling worries (e.g., [18]), cybersecurity conversations were not common in the home environment (e.g., [39]), and children were challenged on their knowledge of cybersecurity when this was shared (e.g. after a school lesson). At school, it became apparent that, for our sample, cybersecurity lessons were treated as 'special' one-off lessons and revisited at specific points in time (e.g., during Internet Safety Day) rather than being reinforced throughout the year.

## **5.3 RQ3: What are young people's preferences for learning cybersecurity concepts?**

Young people appreciated the technical demonstrations of cybersecurity attacks, and expressed an interest in experiencing more of these as well as viewing more pre-recorded videos. In particular, these demonstrations fed their curiosity for the subject, an important aspect for learning [15], and in fact generated more questions around the motivation of the attacker as well as the aftermath of the attack, and thus offered more opportunities for engagement and knowledge transfer. In particular, we gauge some of the effectiveness of the demonstrations by looking at the lowest performing item in the questionnaire post-workshop: software updates. This was the only cybersecurity concept to not be covered with a demonstration during the workshop session and achieved significantly lower scores than the other topics that included demonstrations.

Hand-on activities were also strongly desired, in particular a recreation of the security demonstrations where they can learn both the technical skills but also learn how protective mechanisms (e.g., 2FA) work. The overwhelming majority of participants were keen to perform these activities in groups with friends (supporting more general work on collaborative learning, e.g. [36]). Finally, young people found formal peer support valuable in helping the content be more relatable, in line with similar community initiatives [28]. More work is needed in order to understand the best methods for recruiting and training these pupils, but to also understand the social dynamics at play in a school environment that may promote or prevent the sharing amongst peers.

## **5.4 Converting Good Knowledge to Good Practice**

It was clear from our workshops, albeit through self-reporting, that young people still engaged in poor cybersecurity behaviours despite having good mental models of those security threats (e.g., reusing passwords despite understanding the problems). While similar observations have been reported in the past – in particular when looking at password management [7] – here we go a step further by exploring possible motivations (or lack thereof) for not converting that good knowledge into good practice.

Young people in our workshops reported an expectation that a security compromise would be imminent in their future, and as a consequence they were more relaxed about using security tools or enacting security behaviours – similar to arguments made for privacy fatigue [14]. This potential desensitisation to cybersecurity incidents indicates that communications to young people around cybersecurity behaviours and tools may need to bridge this gap by explaining how they mitigate some opportunistic and perhaps specific attacks (e.g., like the demonstration) rather than focusing on simply relaying the same mechanical information.

Additionally, lack of experience appears to play a role in their understanding of the importance of cybersecurity protective behaviours and tools. We have seen how young people adopt tools with good intentions

but then abandon them due to extra effort, but also how some tools are not adopted at all due to their current situation not seeming problematic (i.e., they currently do not have many passwords). These examples here show how educators are missing a trick by not covering technologies like 2FA and password managers that would be easier to adopt at a younger age when setup will be easier due to a smaller volume of codes. With this added focus on promoting tools, a drive towards continuous reinforcement, as suggested by our participants and as demonstrated in the case of phishing training [20], could help convert knowledge to practice.

### **5.5 Supporting Teachers with Demonstrations and Hands-On Activities**

In this paper we report how presenting young people with technical demonstrations depicting cybersecurity attacks can be an engaging way of starting conversations around this topic. While setting up and running technical demonstrations may be possible for some school teachers (i.e., IT and Computing Science), many other may not possess the skills to properly understand these attacks or to successfully talk through the technical aspects (e.g. [6,26]). Here we have to consider how technical security demonstrations, as well as hands on activities like those described by our participants, could be made more accessible to all teachers given the nature of the DCC. When looking closely at the literature on student learning through modelling, we can see that the use of pre-recorded demonstrations can also be an effective way to convey the key aspects of demonstrations, in many cases resulting in indistinguishable differences when compared with live versions [35]. Therefore, a repository of accessible pre-recorded demonstration content may be a viable avenue for future work. However, supporting hands on practical activities where pupils try out some attacks can be more difficult to support in a safe environment, and more work needs to be done to see whether we can develop plug and play tools that can limit any potential damage to both the pupils and their environment.

## **6 CONCLUSION**

This paper has reported on two full-day workshop sessions with 50 school children aged 12-14 where we explored their existing knowledge of cybersecurity topics and co-designed a cybersecurity lesson. We found that our young participants were keen on the cybersecurity technical presentation depicting different attacks, and these worked both to improve their understanding of the topic but also to encourage further questions around pre-attack and post-attack clarifications. We suggest using these as part of cybersecurity lessons to engage pupils, but also note that pre-recorded demonstrations and videos can serve a similar purpose for educators not comfortable with technical tools. We also found that young people were keen on having more formal peer-to-peer support in schools that could make cybersecurity experiences more relatable. Finally, we suggest that more work should explore how cybersecurity protective tools (e.g. password managers, 2FA, etc.) can be introduced to young people in the early stages of education to encourage their uptake, and support their use, and ensure that their good knowledge of cybersecurity can be translated to actual positive behaviours.

## **ACKNOWLEDGEMENTS**

We would like to thank the young people who took part in in this project, and the school staff who supported them. We would also like to extend our thanks to Reaching Wider at Swansea University for promoting the workshops and organizing school participation and transport. We are grateful to Angharad Devereux for her support in the data collection and initial analysis. Finally, we would like to thank CHERISH DE (EPSRC: EP/M022722/1) at Swansea University for funding the Hard 2 Hack project.



## REFERENCES

1. Murat Akçayır, Hakan Dündar, and Gökçe Akçayır. 2016. What makes you a digital native? Is it enough to be born after 1980? *Computers in Human Behavior* 60: 435–440. <https://doi.org/10.1016/j.chb.2016.02.089>
2. Yusuf Albayram, Mohammad Maifi Hasan Khan, and Michael Fagan. 2017. A Study on Designing Video Tutorials for Promoting Security Features: A Case Study in the Context of Two-Factor Authentication (2FA). *International Journal of Human-Computer Interaction* 33, 11: 927–942. <https://doi.org/10.1080/10447318.2017.1306765>
3. Wei Bai, Michael Pearson, Patrick Gage Kelley, and Michelle L. Mazurek. 2020. Improving Non-Experts' Understanding of End-to-End Encryption: An Exploratory Study. In *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS PW)*, 210–219. <https://doi.org/10.1109/EuroSPW51379.2020.00036>
4. Ahmad Basheer, Muhamad Hugerat, Naji Kortam, and Avi Hofstein. 2016. The Effectiveness of Teachers' Use of Demonstrations for Enhancing Students' Understanding of and Attitudes to Learning the Oxidation-Reduction Concept. *Eurasia Journal of Mathematics, Science and Technology Education* 13, 3: 555–570. <https://doi.org/10.12973/eurasia.2017.00632a>
5. Virginia Braun and Victoria Clarke. 2006. Using thematic analysis in psychology. *Qualitative Research in Psychology* 3, 2: 77–101. <https://doi.org/10.1191/1478088706qp063oa>
6. Moonsun Choi, Dean Cristol, and Belinda Gimbert. 2018. Teachers as digital citizens: The influence of individual backgrounds, internet use and psychological characteristics on teachers' levels of digital citizenship. *Computers & Education* 121: 143–161. <https://doi.org/10.1016/j.compedu.2018.03.005>
7. Yee-Yin Choong, Mary F Theofanos, Karen Renaud, and Suzanne Prior. 2019. "Passwords protect my stuff"—a study of children's password practices. *Journal of Cybersecurity* 5, 1. <https://doi.org/10.1093/cybsec/tyz015>
8. Yee-Yin Choong, Mary Theofanos, Karen Renaud, and Suzanne Prior. 2019. Case Study – Exploring Children's Password Knowledge and Practices. In *Proceedings 2019 Workshop on Usable Security*. <https://doi.org/10.14722/usec.2019.23027>
9. Jasper Cole, Greg Walsh, and Zach Pease. 2017. Click to Enter: Comparing Graphical and Textual Passwords for Children. In *Proceedings of the 2017 Conference on Interaction Design and Children (IDC '17)*, 472–477. <https://doi.org/10.1145/3078072.3084311>
10. Sauvik Das, Laura A. Dabbish, and Jason I. Hong. 2019. A Typology of Perceived Triggers for End-User Security and Privacy Behaviors. 97–115. Retrieved June 10, 2021 from <https://www.usenix.org/conference/soups2019/presentation/das>
11. Iulia Ion, Rob Reeder, and Sunny Consolvo. 2015. "...No one Can Hack My Mind": Comparing Expert and Non-Expert Security Practices. 327–346. Retrieved June 11, 2021 from <https://www.usenix.org/conference/soups2015/proceedings/presentation/ion>
12. Carrie James, Emily Weinstein, and Kelly Mendoza. 2019. *Teaching Digital Citizens in Today's World: Research and Insights Behind the Common Sense K–12 Digital Citizenship Curriculum*. Common Sense Media. Retrieved October 29, 2020 from [https://www.researchgate.net/profile/Donia\\_Ragab/publication/337447543\\_Teaching\\_Digital\\_Citizens\\_in\\_Today's\\_World\\_Research\\_and\\_Insights\\_Behind\\_the\\_Common\\_Sense\\_K-12\\_Digital\\_Citizenship\\_Curriculum/links/5dd82852458515dc2f43a28c/Teaching-Digital-Citizens-in-Todays-World-Research-and-Insights-Behind-the-Common-Sense-K-12-Digital-Citizenship-Curriculum.pdf](https://www.researchgate.net/profile/Donia_Ragab/publication/337447543_Teaching_Digital_Citizens_in_Today's_World_Research_and_Insights_Behind_the_Common_Sense_K-12_Digital_Citizenship_Curriculum/links/5dd82852458515dc2f43a28c/Teaching-Digital-Citizens-in-Todays-World-Research-and-Insights-Behind-the-Common-Sense-K-12-Digital-Citizenship-Curriculum.pdf)
13. Hilda K. Kabali, Matilde M. Irigoyen, Rosemary Nunez-Davis, Jennifer G. Budacki, Sweta H. Mohanty, Kristin P. Leister, and Robert L. Bonner. 2015. Exposure and Use of Mobile Media Devices by Young Children. *Pediatrics* 136, 6: 1044–1050. <https://doi.org/10.1542/peds.2015-2151>
14. Mark J. Keith, Courtenay Maynes, Paul Benjamin Lowry, and Jeffrey Babb. 2014. Privacy Fatigue: The Effect of Privacy Control Complexity on Consumer Electronic Information Disclosure. In *International Conference on Information Systems (ICIS 2014)*. Retrieved July 23, 2018 from <https://papers.ssrn.com/abstract=2529606>
15. John M. Keller. 1987. Strategies for stimulating the motivation to learn. *Performance + Instruction* 26, 8: 1–7. <https://doi.org/10.1002/pfi.4160260802>
16. Agnieszka Kitkowska, Mark Warner, Yefim Shulman, Erik Wästlund, and Leonardo A. Martucci. 2020. Enhancing Privacy through the Visual Design of Privacy Notices: Exploring the Interplay of Curiosity, Control and Affect. 437–456. Retrieved June 10, 2021 from <https://www.usenix.org/conference/soups2020/presentation/kitkowska>
17. Daniel G. Krutka and Jeffrey P. Carpenter. 2017. Digital Citizenship in the Curriculum. *Educational Leadership* 75, 3: 50–55.
18. Priya Kumar, Shalmali Milind Naik, Utkarsha Ramesh Devkar, Marshini Chetty, Tamara L. Clegg, and Jessica Vitak. 2017. "No Telling Passcodes Out Because They're Private": Understanding Children's Mental Models of Privacy and Security Online. *Proceedings of the ACM on Human-Computer Interaction* 1, CSCW: 64:1-64:21. <https://doi.org/10.1145/3134699>
19. Dev Raj Lamichhane and Janet C. Read. 2017. Investigating Children's Passwords Using a Game-based Survey. In *Proceedings of the 2017 Conference on Interaction Design and Children (IDC '17)*, 617–622. <https://doi.org/10.1145/3078072.3084333>
20. Elmer Lastdrager, Inés Carvajal Gallardo, Pieter Hartel, and Marianne Junger. 2017. How Effective is Anti-Phishing Training for Children? In *Thirteenth Symposium on Usable Privacy and Security (SOUPS) 2017*, 229–239.
21. Sumbal Maqsood, Robert Biddle, Sana Maqsood, and Sonia Chiasson. 2018. An Exploratory Study of Children's Online Password Behaviours. In *Proceedings of the 17th ACM Conference on Interaction Design and Children (IDC '18)*, 539–544. <https://doi.org/10.1145/3202185.3210772>
22. Florence Martin, Tuba Gezer, and Chuang Wang. 2019. Educators' Perceptions of Student Digital Citizenship Practices. *Computers in the Schools* 36, 4: 238–254. <https://doi.org/10.1080/07380569.2019.1674621>
23. Florence Martin, Tuba Gezer, Wei Chao Wang, Teresa Petty, and Chuang Wang. 2020. Examining K-12 educator experiences from digital citizenship professional development. *Journal of Research on Technology in Education* 0, 0: 1–18. <https://doi.org/10.1080/15391523.2020.1815611>

24. James Nicholson, Lynne Coventry, and Pam Briggs. 2013. Age-related performance issues for PIN and face-based authentication systems. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '13)*, 323–332. <https://doi.org/10.1145/2470654.2470701>
25. James Nicholson, Lynne Coventry, and Pam Briggs. 2018. Introducing the Cybersurvival Task: Assessing and Addressing Staff Beliefs about Effective Cyber Protection. In *Proceedings of Symposium on Usable Privacy and Security (SOUPS) 2018*, 16.
26. James Nicholson, Youstra Javed, Matt Dixon, Lynne Coventry, Opeyemi Dele-Ajayi, and Philip Anderson. 2020. Investigating Teenagers' Ability to Detect Phishing Messages. In *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 10. <https://doi.org/10.1109/EuroSPW51379.2020.00027>
27. James Nicholson and Jill McGlasson. 2020. CyberGuardians: Improving Community Cyber Resilience Through Embedded Peer-to-Peer Support. In *Companion Publication of the 2020 ACM Designing Interactive Systems Conference (DIS' 20 Companion)*, 117–121. <https://doi.org/10.1145/3393914.3395871>
28. James Nicholson, Ben Morrison, Matt Dixon, Jack Holt, Lynne Coventry, and Jill McGlasson. 2021. Training and Embedding Cybersecurity Guardians in Older Communities. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, New York, NY, USA, 1–15. Retrieved June 10, 2021 from <https://doi.org/10.1145/3411764.3445078>
29. Christos K. Nikopoulos and Mickey Keenan. 2004. Effects of Video Modelling on Training and Generalisation of Social Initiation and Reciprocal Play by Children With Autism. *European Journal of Behavior Analysis* 5, 1: 1–13. <https://doi.org/10.1080/15021149.2004.11434227>
30. Joanne Orlando. Kids need to learn about cybersecurity, but teachers only have so much time in the day. *The Conversation*. Retrieved June 10, 2021 from <http://theconversation.com/kids-need-to-learn-about-cybersecurity-but-teachers-only-have-so-much-time-in-the-day-112136>
31. Al Pascual and Kyle Marchini. 2018. *2018 Child Identity Fraud Study*. Javelin. Retrieved October 29, 2020 from <https://www.javelinstrategy.com/coverage-area/2018-child-identity-fraud-study>
32. Sarah Pearman, Jeremy Thomas, Pardis Emami Naeini, Hana Habib, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, Serge Egelman, and Alain Forget. 2017. Let's Go in for a Closer Look: Observing Passwords in Their Natural Habitat. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS '17)*, 295–310. <https://doi.org/10.1145/3133956.3133973>
33. Emilee Rader, Rick Wash, and Brandon Brooks. 2012. Stories As Informal Lessons About Security. In *Proceedings of the Eighth Symposium on Usable Privacy and Security (SOUPS '12)*, 6:1-6:17. <https://doi.org/10.1145/2335356.2335364>
34. Carlo Sugatan and Florian Schaub. 2020. Interactive Stories for Security Education: A Case Study on Password Managers. In *USENIX Symposium on Usable Privacy and Security (SOUPS) 2020*, 6.
35. Hamidreza Taheri-Torbati and Mohammad Saber Sotoodeh. 2019. Using video and live modelling to teach motor skill to children with autism spectrum disorder. *International Journal of Inclusive Education* 23, 4: 405–418. <https://doi.org/10.1080/13603116.2018.1441335>
36. E. Vass. 2002. Friendship and collaborative creative writing in the primary classroom. *Journal of Computer Assisted Learning* 18, 1: 102–110. <https://doi.org/10.1046/j.0266-4909.2001.00216.x>
37. Rick Wash. 2010. Folk models of home computer security. In *Proceedings of the Sixth Symposium on Usable Privacy and Security (SOUPS '10)*, 1–16. <https://doi.org/10.1145/1837110.1837125>
38. Rick Wash, Emilee Rader, Ruthie Berman, and Zac Wellmer. 2016. Understanding Password Choices: How Frequently Entered Passwords Are Re-used across Websites. 175–188. Retrieved April 14, 2021 from <https://www.usenix.org/conference/soups2016/technical-sessions/presentation/wash>
39. Hue Watson, Eyitemi Moju-Igbene, Akanksha Kumari, and Sauvik Das. 2020. "We Hold Each Other Accountable": Unpacking How Social Groups Approach Cybersecurity and Privacy Together. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (CHI '20)*, 1–12. <https://doi.org/10.1145/3313831.3376605>
40. Jun Zhao, Ge Wang, Carys Dally, Petr Slovak, Julian Edbrooke-Childs, Max Van Kleek, and Nigel Shadbolt. 2019. 'I make up a silly name': Understanding Children's Perception of Privacy Risks Online. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI '19)*, 1–13. <https://doi.org/10.1145/3290605.3300336>
41. Yixin Zou, Kevin Roundy, Acar Tamersoy, Saurabh Shintre, Johann Roturier, and Florian Schaub. 2020. Examining the Adoption and Abandonment of Security, Privacy, and Identity Theft Protection Practices. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (CHI '20)*, 1–15. <https://doi.org/10.1145/3313831.3376570>