SOK: young children's cybersecurity knowledge, skills & practice: a systematic literature review

Maria L. Lamond
Karen V. Renaud
Lara A. Wood
Suzanne Prior

SOK: Young Children's Cybersecurity Knowledge, Skills & Practice: A Systematic Literature Review

Maria. L. Lamond
ABERTAY UNIVERSITY m.lamond2000@abertay.ac.uk

KAREN. V. RENAUD.
UNIVERSITY OF STRATHCLYDE Karen.Renaud@strath.ac.uk

LARA. A. WOOD
ABERTAY UNIVERSITY lara.wood@abertay.ac.uk

SUZANNE. PRIOR
ABERTAY UNIVERSITY s.prior@abertay.ac.uk

The rise in children's use of digital technology highlights the need for them to learn to act securely online. Cybersecurity skills require mature cognitive abilities which children only acquire after they start using technology. As such, this paper explores the guidance and current curriculum expectations on cybersecurity aspects in Scotland. Additionally, a systematic review was undertaken of the literature pertaining to cybersecurity education for children on a wider scale including papers from around the world, with 27 peer reviewed papers included in the final review. We discovered that most research focused on assessing children's knowledge or investigating the efficacy of interventions to improve cybersecurity knowledge and practice. Very few investigated the skills required to carry out the expected cybersecurity actions. For example, high levels of literacy, mature short- and long-term memory, attention, and established meta cognition are all pre-requisites to be able to carry out cybersecurity activities. Our main finding is that empirical research is required to explore the ages at which children have developed essential cognitive abilities and thereby the potential to master cybersecurity skills.

CCS Human Computer Interaction (HCI)

Additional Keywords and Phrases: Children, Password Practice, Authentication, Cognition, Education

1 INTRODUCTION

Children are increasingly using digital technology from an early age [11] and are being described as digital natives; a generation with online access from birth [17]. Digital technology plays a considerable part of children's daily life, both at home and in education [3,45]. The prevalence of online activity is considerable, the most recent figures from Ofcom [39] show that 50% of five –seven -year-olds are playing online games and one in three using online messaging, social media, and live streaming sites or apps. There is a rise in usage of eight–eleven-year-olds, 78% are playing online games, 44% use social media, 64% use online messaging, and with half of 10-year-olds owning their own mobile phone and one third

of six-year-olds [39]. While digital technology use has positive outcomes, presenting new opportunities, and contributing to creativity, it does pose cyber risks from a security and privacy perspective [56, 15]. To mitigate against these risks, it is important that individuals are aware of good cybersecurity practice. This is especially true of young children who are particularly vulnerable to online risks [39, 31], given their lack of knowledge and skills to act safely and securely online. Recent research recommends that cybersecurity education should be as essential as "the three Rs" (reading, writing and arithmetic) [57]. However, it has been acknowledged that lessons on digital privacy and security are rare, particularly for young children, because they are often considered to be unnecessary [25].

Children's cybersecurity education is a multifaceted and multidisciplinary concern. Many stakeholders are responsible for protecting children online, including governments, schools, family, and providing children with the knowledge and skills to protect themselves [23]. There are many considerations for appropriate guidance and educational frameworks, primarily related to the curriculum being developmentally age appropriate [42]. Even so, best practice within cybersecurity, such as creating and authenticating strong passwords, is cognitively challenging for young children in several ways. Password-related cognitive skills include: a level of literacy [14]; problem-solving abilities [48]; ability to pay focused attention [53] and short- and long-term memory [2, 47]. To authenticate using a password, requires retrieving the password from long-term memory, holding it in their working memory (WM), this is cognitively demanding process, often in a noisy and distracting environment.

Passwords must also be kept secret, which requires children to have developed an understanding of the knowledge state and intentions of others [25]. Research suggests that password sharing among children is commonplace but also context dependent [26], and there is also evidence of children knowing this password management rule [1], confirming that children are aware of the importance of password secrecy, but that they do not always do this in practice [47]. Identifying when children have the prerequisite skills to act securely online is important, in terms of providing the right levels of guidance and in deciding what aspects to teach them, whilst acknowledging their online risks. If children use passwords before they are cognitively ready, this increases the likelihood that they will adopt poor password practices that will then continue fostering an insecure cybersecurity culture [2].

This paper reports on a systematic literature review that was undertaken to explore the current landscape of cybersecurity research related to children's cybersecurity knowledge and behaviours. We aimed to answer the following research questions:

RQ1. What cybersecurity guidance and resources are offered to teachers and schools in Scotland and the rest of United Kingdom?
RQ2. Internationally, what cybersecurity knowledge is possessed by young children, their parents, and teachers?
RQ3. Internationally, what interventions have been trialled to improve cybersecurity knowledge and skills in young children?
RQ4. Internationally, what cognitive abilities scaffold the learning and practice of cybersecurity skills?

2 METHODOLOGY

To answer RQ1, we decided to focus on one country with a national curriculum, because that removed any potential confounds caused by varying curricula and differing government-led approaches to raising cyber awareness, knowledge, and skills in children. This also eliminates the noise that would deter analysis if we attempted to review the entire world's curricula. We chose Scotland as our country given that it satisfies these requirements but also because Education Scotland publishes a great deal of information which we could use to inform our review. As such, we reviewed the grey literature related to Scottish curricula including online websites, articles, and government documents such as: the curriculum for

excellence, policy documents, and strategic frameworks, all of which pertain to advice and guidance on cybersecurity education specific to Scottish primary schools.

To answer the rest of the research questions, a systematic literature review of academic databases was conducted following the guidelines created by the Preferred Reporting Items in Systematic reviews and Meta Analysis (PRISMA) [19]. The process included defining appropriate keywords, the years to delineate the search, the inclusion/exclusion criteria, and the databases to be searched. All articles were reviewed for inclusion, extracting data required by the research questions, and synthesising the insights obtained from the papers. Figures 1 and 2 show Prisma diagrams for the grey literature and academic database searches, respectively. Table 1 in the appendix displays the full inclusion and exclusion criteria.

Figure 1

Grey Literature Prisma Data Collection Diagram

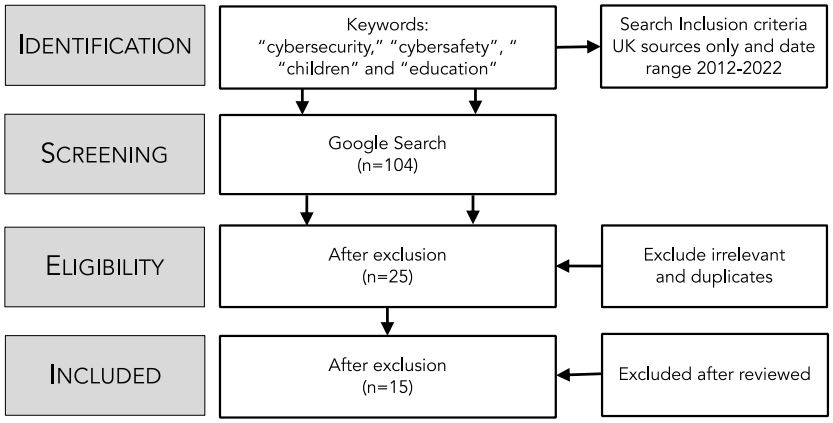
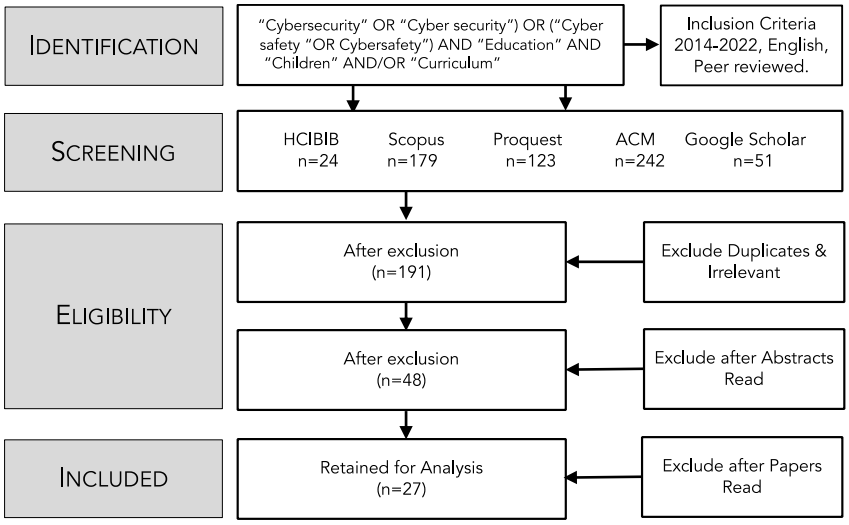


Figure 2

Prisma Data flow Diagram



2.1 Systematic literature review characteristics

Table 2

Systematic literature review paper characteristics

	Knowledge & Attitudes N =14	Interventions N =13
Participants		
Children	13	13
Parents	6	1
Teachers	2	
Sample Size		
N <25	3	4
N >25-50	4	6
N>50-100	1	2
N>100	6	1
Year		
2014-2016	1	1
2017-2019	8	8
2020-2022	5	4

N= number of papers

The papers addressed cybersecurity knowledge and attitudes as well as cybersecurity interventions. Table 2 displays research characteristics, all research papers included children except one that focused on educators' experiences. Parents were included in seven papers and teachers in two. Papers that sought knowledge and attitudes were more likely to include larger sample sizes and use survey or interview research methods. The papers that addressed participants' knowledge identified their awareness of cybersecurity risks and assessed their cybersecurity skills for example creating strong passwords or identifying phishing emails. Papers that reflected participants' attitudes referred to the participants feelings towards cybersecurity and often sought qualitative responses. For example, Muir and Joinson [36] reported that parents expressed a feeling of limited cybersecurity knowledge but felt they could spot scams online. Papers that focused on assessing cybersecurity interventions were more likely to have smaller sample sizes and use an experimental design. Many papers used more than one method and included children from different age groups. All but one paper analysed the different age groups and therefore allowed for the extraction of data that pertained to the target age group of children between 4 and 12. The majority (89%) of papers are from 2017-2022 although the inclusion was from 2014; this could indicate an increase in research in this area in later years and thus provides a recent overview.

2.2 Analysis Process

The grey literature was synthesized into two categories; the first category included literature such as: government policy documents, frameworks, strategies and curriculum documents (see Appendix Table 4 for a list of all documents). The second included websites that held cybersecurity resources for children, parents and teachers (website details and links can be found in Table 3 in the appendix).

The review of academic papers was first categorised by paper focus where two distinct types emerged; papers that sought children's knowledge, attitudes and practice, and papers that assessed the effectiveness of an intervention to enhance cybersecurity knowledge, awareness or practice**.** The main findings from each paper were synthesized and a narrative account can be found Sections 3.2 and 3.3.

The other research questions were addressed by synthesising the papers that mention different cognitive functions, to identify the distinct functions perceived as being important. Note that some terminology, such as difficulty recalling/remembering, was categorised as "memory", and issues relating to overconfidence in ability was recorded as "meta cognition" (one's perceptions of one's own ability). These cognitive functions were then mapped to password practice; creation, managing and authenticating (see Appendix Figure 4).

3 RESULTS

All resources pertain to Scotland except for a comparison between the UK and Department for England curriculum for cybersecurity due to the same cybersecurity resources being used in Scotland and the greater UK. The findings from the review of the grey literature revealed an inconsistency between curriculum benchmarks, policy and the resources.

3.1 RQ1: What cybersecurity guidance and resources are offered to teachers and schools?

The Curriculum for Excellence (CfE) is Scotland's curriculum for children and young people between the ages of 3-18 with the aim of providing young people with the knowledge and skills for learning. Part of the curriculum includes benchmarks for technologies [16] which provide guidance on building cyber resilience for children in Scotland. The benchmarks contain outcomes linked to cybersecurity knowledge and practice. The current outcomes are set at four developmental levels: early level ages 3-5, first level age 6-8, second level 9-12 and third and fourth levels for secondary education. The outcome at the early level is for children to use a password to log on to a preferred device. At the first level children should be able to use a strong a password and know how to be safe and secure online. The outcomes at these levels do not consider children's developing literacy abilities, typically children are only developing literacy skills at this stage. The cybersecurity outcomes are limited to password knowledge and practice until children are in secondary education, where other concepts such as hacking, phishing and virus protection are introduced.

The online resource be internet legends [21] developed by Parent Zone UK and Google introduces and develops children's knowledge on security aspects such as password creation, but also phishing and hacking through videos and interactive games from age seven. The resource has lesson plans and resources for teachers and parents linked to activity and outcomes (see table 6 in appendix). The "Be Internet Legends" [7] resource exposes an inconsistency between the outcomes and judgements that are advised through the curriculum for teachers, and what is being developed.

3.1.1 Scottish policy and strategic frameworks

There are a number of published strategies and frameworks put forward by the Scottish government to tackle the issue of online risks through developing cyber resilience. The strategy "Safe, Secure and Prosperous" [51] outlines the importance of cyber resilience being taught in learning settings at all ages and stages of education from preschool. The importance of skills being communicated in the right way are highlighted particularly for children and young people. "Cyber resilience

is about individuals and organisations being able to prepare for, withstand, rapidly recover and learn from deliberate attacks or accidental events in the online world." [51, pp 2]. The "National Internet Safety Action Plan for Scotland" [49] highlights developing Internet safety skills from an early age and acknowledges the need for cybersecurity content to be included in online sources and resources. The plan includes cybersecurity content being available as a section within Parent zone Scotland [40], an online website delivered through Education Scotland as a resource for giving parents information on education. This content has become available through the same resource used by Parent zone UK [41] despite the UK and Scotland having different curriculum benchmarks related to digital literacy and security. The Cyber Resilient Scotland: strategic framework [50] has been put forward with a national focus on individuals and workplaces. This has a limited focus on children, but it is aiming to build capacity across school education, achieved through embedding cybersecurity education within the curriculum providing teachers, with support and, guidance that is to be extended to parents and carers. The strategic outcomes are indicated by assessing young people's cybersecurity behaviour and knowledge through the young people in Scotland survey, yet this is only administered to children between the age of 11 to 18.

3.1.2 UK Curriculum

The UK Government has developed their curriculum on cybersecurity with the UK Council for Internet Safety (UKCIS). The guidance is set out in the framework; education in a connected world [19], under the section privacy and security. The privacy and security section explores how personal online information can be used, stored, processed, and shared**.** The outcomes for children between the ages of 4-7 are simple; an introduction to the concept of private information and who you can share private information with such as trusted adults. Similar to the Scottish curriculum, children should be able to explain that passwords are needed to protect personal information. The UK guidance, however, makes no demands that young children can use passwords, only that they are beginning to understand password rules on creating and protecting passwords. It is not until much later that children would be expected to demonstrate password use and this is in contradiction with Scottish guidance. The UK curriculum outcomes contain a more detailed and advanced approach to cybersecurity education including aspects of phishing and scams between the ages of 7-11. The outcomes related to being able to describe what a phishing attack is and have strategies to help identify such content**.** UKCIS provides a more detailed comprehensive list of outcomes that could be objectively measured unlike the CfE where outcomes are limited.

3.1.3 Online resources for children, parents and teachers

Online resources specific to Scotland and the UK (see Table 5 in appendix) either have cybersecurity resources or signposts to relevant resources. Online sites such as Think U know [54] and Internet Matters [21] that are predominantly related to cybersafety direct to the *National Cyber Security Centre* (NCSC) [37]. The NCSC provides resources for children aged 7-11 with activities for schools and at home that focus on how to create strong passwords, identifying suspicious messages, what emails should look like, and a section on investigating phishing. NCSC have developed an interactive game "cyber sprinters" where children can practice being cybersecure by running through cyberspace and unlocking padlocks by answering cybersecurity questions correctly such as 'you receive a message from someone you don't know with a link, would you click on the link'. The resource "Be Internet Legends" [7] contains resources that can be used in the home and in class aimed at children aged 7-11. Be Internet Legends contains several age-appropriate lesson plans for ages 7-9 and 9-11, is aligned with framework education in a connected world [19] and follows the curriculum outcomes. The resource is defined as improving online safety and provides resources related to cybersafety yet also includes cybersecurity aspects. The cybersecurity aspects include being alert and secure involving hacking, phishing, and how to create strong passwords. The guidance on how to create a password including special characters, numbers, and a mix of lower and upper case does not align with current guidance on creating passphrase passwords (NCSC) [37]. Similar to the game developed by NCSC, Be Internet Legends has a game, *Interland,* that allows children to combat badly behaved hackers and phishers to remain secure. The game requires children to make passwords or identify hacking attacks with immediate feedback, which provides good learning and awareness opportunities.

3.2 RQ2: What cybersecurity knowledge is possessed by young children, their parents and teachers? (*Paper IDs: P3, P4, P5, P25).*

Lorenz *et al.* [32] ran a large survey with Estonian children from age nine to 14 and reported that despite 97% owning their own mobile devices, laptops, or iPads, 34% do not use passwords or PINs, and 56% choose a WIFI network to access the internet that could put their device at risk from hacking and malware. When asked what safe technology was, one fifth of 4th grade students aged nine- to 10-years-old lacked the skills or understanding to answer this question. Assal *et al.* [6] interview data with children aged 8-15 displayed limited awareness of security practices, with the majority relying on parental support for managing their passwords. Tirumala *et al.* [55] found similar gaps in knowledge of younger children related to cybersecurity awareness, only 1% of 8–12-year-olds were aware of phishing despite it being one of the most significant threats. A phishing awareness intervention was explored by Lastdrager *et al.* [29], in their pre-test evaluations, reported that children between the age of 9 and 12 displayed mediocre abilities to discriminate between phishing emails/fake websites versus legitimate ones.

3.2.1 Subjective versus objective knowledge (Paper IDs: P20, P21, P22)

Objective knowledge refers to the actual knowledge or skill children hold, whereas subjective knowledge refers to perceived or self-assessed knowledge. Researchers identified an inconsistency between subjective and objective knowledge on cybersecurity [11, 47, 33]**.** Macaulay *et al.* [33] assessed subjective versus objective knowledge and attitudes to online safety. The paper focused on cybersafety but as this included computer viruses, we include it here. Findings showed a significant association between subjective knowledge and perceived online safety but only a weak association between subjective and objective knowledge. Choong *et al.* [11] investigated password knowledge, perceptions, and practice, despite children reporting they found it easy to create passwords, their passwords were not strong. Ratakonda *et al.* [47] confirmed that both adults and children did not use their theoretical knowledge in the practice of password creation, despite having subjective knowledge of good password practice.

3.2.2 Children have poor password practice (Paper IDs: P6, P12, P18, P22, P34b).

Lamichhane and Read [28] used an app to explore password creation by children aged 7-8, finding that many participants created simple usernames and passwords and tended to make spelling mistakes when typing. Choong *et al.* [12] illustrated that password strength was poorer in elementary school children, with 31% using letters only. This in and of itself does not indicate that the passwords are weak – if they were using three random words this would be fine, but this is unlikely to be the case [28]. Masqsood *et al.* [34b] similarly found weak passwords, where children created passwords that contained self-relevant information such as their names.

Children's passwords are often created for them by parents or teachers [11, 12, 23]. Kumar *et al.* [11, 25] identify the secrecy of passwords as being context dependent on family, friends, and education. Parent's showed variation and uncertainty over who children should share passwords, with consideration given to age and capabilities. Kumar, *et al.*'s [25] findings suggested that children aged 5-9 did not understand the associated risks with sharing password information and failed to recognise privacy and security threats. Choong *et al.* [11, 12] found that a high percentage of all children, irrespective of age group, understood the importance of password secrecy, yet older children are more likely to share passwords with their friends and use the same password for everything. Moreover, younger children were more likely to write their passwords down and were more likely to ask family members to remember them.

3.2.3 Parents and teachers' knowledge and attitudes towards cybersecurity (Paper IDs: P2, P5, P7 P9, P15, P25, P26).

Muir and Joinson [36] and Kumar *et al.* [27] show that parents use a variety of strategies to mediate security threats from setting boundaries and rules, monitoring use to communicating and educating. Parents typically use passive strategies that include setting boundaries, controls and rules, reporting that they did not feel their children were at a security risk and would tackle security concerns at a later stage. Some parents also felt they had limited security knowledge, and displayed

poor password hygiene, yet they play a significant role in children's development of cybersecurity knowledge and practice [6, 27, 34 36]. Hundlani *et al.* [20] found that parents resorted to coping strategies around children's password practice such as writing down passwords or not using them due to their children repeatedly forgetting their passwords and locking themselves out of devices. Research with teachers showed that they are required to help students to manage their passwords but have a lack of training around cybersecurity. Teachers are often given training in new technologies but with no security or privacy considerations [26]. Kumar *et al's.* [26] study with teachers and educators found that lessons on privacy and security online for children were rare, with some reporting that these were not necessary for young children, and found it difficult to incorporate cybersecurity lessons due to all their other teaching demands. Renaud and Prior [42] found a conflation between teachers' and children's understanding of security versus safety in relation to the purpose of having a password, and this conflation of terms has been apparent in many of the papers in this review. Lorenz *et al.* [32] suggest that teachers, parents, and students themselves all have responsibility to ensure children learn and practice cybersecurity and cybersafety.

3.3 RQ3: What interventions have been trialled to improve cybersecurity knowledge and skills in young children?

This review paper identified 13 papers that included an intervention to enhance cybersecurity knowledge or practice. The papers fell into three broad categories related to (1) passwords, (2) phishing, (3) general cybersecurity aspects, usually combined with cybersafety topics.

3.3.1 Graphical Passwords (Paper IDs: P11, P13, P23, P25).

Alkhamis *et al*. [2] study found that children between the age of 6-9 were able to effectively authenticate with a doodle they created, and this persisted in subsequent trials. Assal *et al.* [6] assessed usability and preference for graphical passwords for children and adults, finding a preference for graphical authentication, with children most effectively recalling distinct objects like an animal, this was also found by Stewart *et al*. [53] in their study with younger children. Cole *et al.* [14] found conflicting evidence suggesting that both children aged 6-12, and adults had less success using graphical passwords, despite them being more memorable in the short term.

3.3.2 Phishing Interventions (Paper IDs: P4, P16).

Very few papers investigated young children's phishing knowledge and practice. Alwanin [4] conducted an experiment to assess the impact of anti-phishing training on the popular application WhatsApp on children aged 7-13 and found a significant positive effect, yet there was not a significant difference between the control group and the intervention group. Lastdrager *et al.* [29] similarly tested the impact of an intervention to help children spot phishing messages with positive findings. However, the impact diminished over time to match that of the control group by week 4. Children that had their own personal email addresses were more likely to spot phishing messages.

3.3.3 Cybersecurity web-based learning (Paper ID: P1, P2, P14, P27).

Several papers investigated the effects of online web games or apps to improve cybersecurity knowledge [1, 18, 34, 38, 47] Giannakas *et al.* [18] designed an app "Cyberaware" specifically for elementary students based on the Attention, Relevance, Confidence and Satisfaction (ARCS) model of motivation [24], where students are motivated to participate and learn due to intrinsic interest. The intervention group showed an improvement in their scores by 20% which was significantly greater than scores of the control group. Nicolaidou and Venizelou [47] similarly used an interactive web-based game "be smart when online" and found a large effect size indicating it as an effective resource to improve cybersecurity knowledge, however the sample size was small. Maqsood *et al.* [34] web-based game used procedural rhetoric, in that the learners discover the arguments through experience in scenarios rather than it being presented as information. Children's knowledge and behaviour intention scores from the pre-post-test improved significantly and they

retained this knowledge in a further post week assessment. Again, the sample size was small but provided pedagogical advice for the learning of cybersecurity knowledge including, realistic narrative and age-appropriate scenarios.

3.3.4 Novel cybersecurity interventions (Paper IDs: P8, P17, P24).

Three papers provide a novel approach to teaching children about cybersecurity. Reid and Van Niekerk [48] adapted the traditional snakes and ladders board game to teach children about password creation and sharing, using Brain Compatible Education (BCE) through promoting the attention and processing by the learner (Caine and Caine, 1991) [8]. Post-game surveys displayed an improvement in password management practices, including who to share your password with improved from 26% to 73% in children aged 9-11. Chartoflylaka and Delcroix [9] explored the effectiveness of including password rules in a storytelling game activity. In creating the story and using words from this game, the children were able to produce longer passwords. Jeong and Chiasson [22] addressed children's perceptions of cybersecurity warnings and found ambiguity of some warnings to be a concern and the need for cybersecurity warnings to be clearer, less ambiguous, and suggests that colours alone did not provide enough information.

3.4 RQ4: What cognitive abilities scaffold the learning and practice of cybersecurity skills? *(Paper IDs: 1, 2, 8, 11, 12, 18, 19, 21, 25).*

Most papers propose developing cognitive functions such as: memory; attention; meta cognition; literacy; and social cognition as being responsible for children's difficulties with cybersecurity skills, particularly around password practice. Figure 1 (see appendix) shows the prevalence of various cognitive functions being mentioned in the literature and Figure 2 (see appendix) displays the cognitive functions in relationship to password practice, as reported by the papers in this review.

The papers suggest a number of potential cognitive functions that may limit children's ability to create password. Stewart *et al.* [53] identifies children's limitations with literacy as a problematic for young children as they may be unable to yet make words to create passwords, additionally keyboard use can be challenging given the letters are uppercase yet produces a lowercase letter. Children are seen to make spelling mistakes whilst typing to make usernames and passwords as they have chosen passwords that they are not confident in spelling [28]. Choong *et al.* [12] report that children frequently use personal information in password creation. This is a common theme in the literature which illustrates insecure behaviour and may suggest difficulties in problem solving or critical thinking to create a strong password. This is further supported by Maqsood *et al.* [34] with results indicating that even children ages 11-13 create simple and self-relevant passwords. Assal *et al.*'s [6] study explore authentication practices of children and observed that they had trouble memorising their passwords when words were used and stated that children's skills and cognitive abilities must be considered. As alternative authentication methods for children are the most prevalent intervention within this review with researchers exploring graphical and picture or doodle type password for children. This endeavour for an alternative password practice for children demonstrates the importance of addressing children's skills and cognitive capacity to create and use passwords securely. Children's attention is considered important in leaning cybersecurity principles, for ensuring processing and extracting meaning [18,48]. Authenticating or inputting a password into a device is problematic for children [6,28]. It is found that when children input a wrong password it was often closely related to the password they created, but not identical. This indicates potential challenges with typing or spelling errors rather than their ability to retain the password.

3.4.1 Younger children show an inflated meta cognition in password practice. (Paper IDs :8, 18, 19 ,21).

A recurring finding illustrated that younger children were more likely to think they could create strong passwords and remember them than older children, suggesting over- or misplaced confidence and a discrepancy between their subjective and objective knowledge [12, 34, 48]. Ratakonda *et al.* [47], found a mismatch between children's understanding and practice, despite being aware of the guidance on how to make a strong password, they did not do so in practice. Similarly, Choong *et al.* [11] reports children's perceptions of their password practice and found the younger group (3rd to 5th) found

it easier to make passwords, make different passwords and remember passwords than their older counterparts (6th-8thgrade). Reid and Van Niekerk's [48] survey before the intervention of an offline game showed that 67% the youngest group 9–11-year-olds reportedly knew how to create a strong password but only 56% of 12- to 14-year-olds knew this. This might be due to recent inclusion of awareness drives in schools, which means that younger children receive instruction that older children did not get, or an overconfidence in what constitutes a strong password.

4 DISCUSSION

4.1 RQ1: Cybersecurity curriculum and guidance

The review suggests that children do not have adequate cybersecurity knowledge and that the Scottish policy and curriculum have not kept up to date with advances and technology or indeed with the advanced use of technology by children. As children are using and owning smart devices from an early age with this trend continuing there is real cybersecurity risk to children. Currently the Scottish curriculum does not include outcomes relating to risks such as phishing and hacking until they are in secondary education. Worryingly, the Scottish curriculum contains early level outcomes that children can log on to a preferred device with a password, but this is outcome is beyond children's developmental capacity at this stage. Literacy is a multifaceted and complex skill that children begin to learn from birth that changes greatly as it develops and between children; children at preschool level are likely to be able to begin to sound letters and recognise letters and simple words and not develop word formation or writing and reading until later (Snow, 2004) [52]. Additionally, the curriculum benchmarks are constricting as they do not provide objective measures of cybersecure practice and limited in their expectations.

The online resources developed by NCSC, Google and Parentzone provide useful resources that aim to equip children with the knowledge and skills they require to be secure online however the age range is wide particularly the NCSC resource is for children aged 7-11 where children will be developmentally different and may require age-appropriate resources. Although there are strategic frameworks developed by the Scottish government to improve cybersecurity the emphasis is on a national level without a strategic focus on young children and how this will be achieved through teachers and schools. Rahman *et al.* [46] review paper explored the importance of cybersecurity education in schools and the strategies stakeholders can implement to promote cybersecurity education finding that despite the clear need for cybersecurity education, teachers do not have the skills or knowledge to currently educate children on cybersecurity aspects. It is evident that cybersecurity education for children must be revolutionised with collaboration from all stakeholders with appropriate funding and resources.

4.2 RQ2: Children display low cybersecurity knowledge and awareness

The review has highlighted a potential discrepancy in children's perceptions or subjective knowledge and their actual knowledge and practice [33]. As many of the papers pertaining to knowledge and practice through self-report measures it may not be giving a true reflection of children's cybersecurity practices and they may not use this theoretical knowledge in practice as seen in Ratakonda *et al.* [47]. As children show an inflated perception of their abilities in cybersecurity skills can leave them susceptible to cyber risks. The review has highlighted issues related to children's perception of ability; further research should be undertaken to ascertain if children choose not to use their theoretical knowledge or if they do not have the cognitive abilities to put this knowledge to practice without support, guidance, or further training. Children learn about cybersecurity from parents and caregivers [6, 26] and rely heavily on their support in creating and managing passwords. Despite this, parents do not act securely and report not having adequate knowledge [30, 32]. The vital role that parents play in establishing children's cybersecurity practice illustrates the importance of educating parents appropriately in cybersecurity education to have confidence when teaching their children [3].

RQ3: Interventions

While the review indicates that interventions are positive in promoting cybersecurity knowledge, objectively measuring how children use this knowledge in practice in difficult to ascertain [1]. Therefore, illustrating a potential gap in the research around children's practice and not only their perceptions of knowledge and practice. The interventions applied a number of psychological theories to the pedagogy of the learning games, and this was seen as useful in creating an effective learning environment. The types of interventions utilised alternative learning strategies through web-based leaning, gamification, and storytelling. This is interesting as it differs from traditional styles of learning. Quayyum *et al.* [45] systematic review on children's cybersecurity awareness suggested research investigating interventions to improve cybesecurity awareness need to be more robust. Furthermore, Quayyum *et al*. [45] recommended research to try more traditional approaches to learning to assess if the alternative strategies are more effective. Further research could be useful in identifying psychological models of learning and identifying age-appropriate development curriculum.

4.3 RQ4: The role of cognition

A unique element of this review focused on the underlying cognitive functioning that may be required in the development of cybersecurity skills. The research to date has proposed potential cognitive functions and whilst the predictions are intuitive, they lack empirical testing. Identification of the associations between the cognitive ability and cybersecurity skill would be beneficial in knowing when the right time is to teach children and for developing strategies to help children with these practices. The papers in this review aligned closely with Choong *et al.* [10] paper, that established a cognitive behavioural framework to understand the password management cycle. Aspects of cognition such as memory and literacy were considered important in the creation of passwords from our review. Choong *et al*. [10] additionally emphasised the importance of problem solving in password generation and why this is a crucial area of investigation for both novices and experts. The papers in this review placed greater importance on memory and literacy whilst potentially overlooking problem solving in password generation which could be vital in solving problems with password generation. Children have been observed to have difficulty with authentication and the research suggests memory, attention, and literacy most prominently, the experiences of authentication may then be often negative for children, and this is proposed as affecting the way in which passwords will then be created in the future [2]. It is likely then, that children will choose to create weak passwords to improve authentication experiences, and thus continuing insecure password practice. It is crucial to change the way passwords are viewed and used and this requires an innovative approach to the teaching and developing of these skills.

5 LIMITATIONS

In answering the first research question, we chose to focus only on Scottish curricula, to examine and analyse one country's approach. We have no reason to believe that it is significantly different from what the rest of the UK and indeed the rest of the world's schools, are doing. Indeed, the UK is ranked 2nd on the Oliver Wyman Global Cyber Risk and Education Index, in terms of their cyber-related educational systems [35]. Even so, we acknowledge that there needs to be a more wide-ranging study to determine whether our findings are reflective of other countries' educational practices.

6 CONCLUSION

This review has provided a current overview of cybersecurity education for young children. While steps are being taken to improve cybersecurity awareness, there is a need for well-defined age-appropriate outcomes, and for teachers and parents to receive adequate training to empower them to protect and teach children cybersecurity principles. The review provided a snapshot of cybersecurity research with children, where agreement is found in the requirement for a more inclusive cybersecurity education, and with the challenges children are confronted with when being cybersafe and cybersecure. Passwords are difficult for children and require several cognitive functions that younger children are still developing. Future work is required to understand children's developing cognition in line with the cybersecurity skills they are expected

to have. Moreover, research developing and accessing interventions to improve awareness on a larger scale, with robust research methodology is also needed.

The review identified potential prerequisite developmental and cognitive abilities that contribute to the learning and practice of cybersecure behaviour. Grey resources pertaining to the guidance and resources on teaching cybersecurity to children were reviewed to establish whether resources and guidance are developmentally appropriate. We found the currently curriculum relating to cybersecurity to be limited and not consistent with where children are developmentally, nor does it take into consideration the risks they face.

REFERENCES

[1] Al Shamsi, A.A., 2019. Effectiveness of cyber security awareness program for young children: A case study in UAE. *Int. J. Inf. Technol. Lang. Stud*, *3*(2), pp.8-29.

[2] Alkhamis, E., Petrie, H. and Renaud, K., 2020, July. KidsDoodlePass: An exploratory study of an authentication mechanism for young children. In International Symposium on Human Aspects of Information Security and Assurance (pp. 123-132). Springer, Cham.

[3] Alqahtani, N., Furnell, S., Atkinson, S. and Stengel, I., 2017, September. Internet risks for children: Parents' perceptions and attitudes: An investigative study of the Saudi Context. In Internet Technologies and Applications (ITA) (pp. 98-103). IEEE.

[4] Alwanain, M.I., 2021. How Do Children Interact with Phishing Attacks?. International Journal of Computer Science & Network Security, 21(3), pp.127-133.

[5] Annansingh, F. and Veli, T., 2016. An investigation into risks awareness and e-safety needs of children on the internet: a study of Devon, UK. Interactive Technology and Smart Education.

[6] Assal, H., Imran, A. & Chiasson, S. 2018, "An exploration of graphical password authentication for children", International Journal of Child-Computer Interaction, vol. 18, pp. 37-46.

[7] Be Internet Legends curriculum_2022. Available at https://storage.googleapis.com/gwebinterland.appspot.com/engball/hub/pdfs/Be%20Internet%20Legends%20curriculum%20_2022.pdf. (Accessed:27/05/21

[8] Caine, R.N. and Caine, G., 1991. Making connections: Teaching and the human brain. ASSOCIATION FOR SUPERVISIONAND CURRICULUM DEVELOPMEN

[9] Chartofylaka, L. and Delcroix, A., 2018, July. StoryPass–Password Rules Hidden in a Storytelling Game Activity: Steps towards Its Implementation. In 8th International Toy Research Association World Conference.

[10] Choong, Y.Y., 2014, June. A cognitive-behavioral framework of user password management lifecycle. In International Conference on Human Aspects of Information Security, Privacy, and Trust (pp. 127-137). Springer, Cham.

[11] Choong, Y.Y., Theofanos, M., Renaud, K. and Prior, S., 2019, February. Case study: exploring children's password knowledge and practices. In Workshop in Usable Security and Privacy. Internet Society. San Diego, United States Duration: 24 Feb 2019 → 27 Feb 2019

[12] Choong, Y.Y., Theofanos, M.F., Renaud, K. and Prior, S., 2019. "Passwords protect my stuff"—a study of children's password practices. Journal of Cybersecurity, 5(1), p.tyz015.

[13] Cole, J., Walsh, G. and Pease, Z., 2017, June. Click to enter: Comparing graphical and textual passwords for children. In Proceedings of the 2017 Conference on Interaction Design and Children (pp. 472-477).9. DOI=https://doi-org.libproxy.abertay.ac.uk/10.1016/j.ijcci.2020.100169.

[14] Cole, J., Walsh, G. and Pease, Z., 2017, June. Click to enter: Comparing graphical and textual passwords for children. In Proceedings of the 2017 Conference on Interaction Design and Children (pp. 472-477).

[15] Da Veiga, A., 2016, July. A cybersecurity culture research philosophy and approach to develop a valid and reliable measuring instrument. In 2016 SAI Computing Conference (SAI) (pp. 1006-1015). IEEE.

[16] Education Scotland. Benchmarks Technologies. 2017. Available at https://education.gov.scot/nih/Documents/TechnologiesBenchmarksPDF.pdf. (Accessed:14/04/2021)
[17] Edwards, S., Nolan, A., Henderson, M., Mantilla, A., Plowman, L. and Skouteris, H., 2018. Young children's everyday concepts of the internet: A platform for cyber-safety education in the early years. British Journal of Educational Technology, 49(1), pp.45-55.
[18] Giannakas, F., Papasalouros, A., Kambourakis, G. and Gritzalis, S., 2019. A comprehensive cybersecurity learning platform for elementary education. Information Security Journal: A Global Perspective, 28(3), pp.81-106.
[19] GOV. UK. Education for a Connected World -2020 edition. Available at https://www.gov.uk/government/publications/education-for-a-connected-world. (Accessed: 08/08/2021)
[20] Hundlani, K., Chiasson, S. and Hamid, L., 2017, September. No passwords needed: The iterative design of a parent-child authentication mechanism. In Proceedings of the 19th international conference on Human-Computer Interaction with Mobile Devices and Services (pp. 1-11).
[21] Internet matters.Information, Advice and Support to Keep Children Safe Online. Available at Https://www.internetmatters.org. (Accessed: 02/06/2021)
[22] Jeong, R. and Chiasson, S., 2020, April. 'Lime','Open Lock', and 'Blocked' Children's Perception of Colors, Symbols, and Words in Cybersecurity Warnings. In Proceedings of the CHI Conference on Human Factors in Computing Systems (pp. 1-13).
[23] Kaban, A., 2021. Secure Internet Use in Information Technologies and Software Course Textbooks at Primary and Secondary Schools. Athens Journal of Education, 8(1), pp.37-52.
[24] Keller, J.M., 1987. Development and use of the ARCS model of instructional design. Journal of instructional development, 10(3), pp. 2-10.
[25] Kumar, P., Naik, S., Devkar, U., Chetty, M., Clegg, T. & Vitak, J. 2017, "No Telling Passcodes Out Because They're Private", Proceedings of the ACM on Human-Computer Interaction (CSCW), vol. 1, pp. 1-21.
[26] Kumar, P.C., Chetty, M., Clegg, T.L. and Vitak, J., 2019, May. Privacy and security considerations for digital technology use in elementary schools. In Proceedings of the CHI Conference on Human Factors in Computing Systems (pp. 1-13).
[27] Kumar, P.C., Subramaniam, M., Vitak, J., Clegg, T.L. & Chetty, M. 2020, "Strengthening Children's Privacy Literacy through Contextual Integrity", Media and Communication (Lisboa), vol. 8(4S2), pp. 175-184.
[28] Lamichhane, D.R. and Read, J.C., 2017, June. Investigating children's passwords using a game-based survey. In Proceedings of the 2017 Conference on Interaction Design and Children (pp. 617-622).
[29] Lastdrager, E., Gallardo, I.C., Hartel, P. and Junger, M., 2017. How Effective is {Anti-Phishing} Training for Children?. In Thirteenth symposium on usable privacy and security (soups 2017) (pp. 229-239).
[30] Liberati, A., Altman, D.G., Tetzlaff, J., Mulrow, C., Gøtzsche, P.C., Ioannidis, J.P., Clarke, M., Devereaux, P.J., Kleijnen, J. and Moher, D., 2009. The PRISMA statement for reporting systematic reviews and meta-analyses of studies that evaluate health care interventions: explanation and elaboration. Journal of Clinical Epidemiology, 62(10), pp. e1-e34.
[31] Livingstone, S., Davidson, J., Bryce, J., Batool, S., Haughton, C. and Nandi, A., 2017. Children's online activities, risks and safety: a literature review by the UKCCIS evidence group.
[32] Lorenz, B., Kikkas, K. & Osula, K. 2018, "Development of Children's Cyber Security Competencies in Estonia" in Learning and Collaboration Technologies. Learning and Teaching Springer International Publishing, Cham, pp. 473-482.
[33] Macaulay, P.J., Boulton, M.J., Betts, L.R., Boulton, L., Camerone, E., Down, J., Hughes, J., Kirkbride, C. & Kirkham, R. 2020, "Subjective versus objective knowledge of online safety/dangers as predictors of children's perceived online safety and attitudes towards e-safety education in the United Kingdom", Journal of Children and Media, vol. 14, no. 3, pp. 376-395.
[34] Maqsood, S., Biddle, R., Maqsood, S. and Chiasson, S., 2018, June. An exploratory study of children's online password behaviours. In *Proceedings of the 17th ACM Conference on Interaction Design and Children* (pp. 539-544).

[34b]Maqsood, S., Mekhail, C. and Chiasson, S., 2018, June. A day in the life of JOS: a web-based game to increase children's digital literacy. In Proceedings of the 17th ACM conference on Interaction Design and Children (pp. 241-252).
[35] Mee, P., Brandenburg, R. and Lin. W. 2021. Oliver Wyman Forum Global Cyber Risk and Education Index. https///www.oliverwymanforum.com/content/dam/oliver-wyman/ow-forum/cyber/index/Oliver-Wyman-Forum-CLE-Index-Methodology-Apr-2021.pdf. Accessed 30 May 2022.
[36] Muir, K. & Joinson, A. 2020, "An Exploratory Study Into the Negotiation of Cyber-Security Within the Family Home", Frontiers in Psychology, vol. 11, pp. 424.
[37] NCSC. Cybersprinters. Available at https://www.ncsc.gov.uk/collection/cybersprinters. (Accessed: 21/5/2021)
[38] Nicolaidou, I. and Venizelou, A., 2020. Improving children's E-safety skills through an interactive learning environment: A quasi-experimental study. Multimodal Technologies and Interaction, 4(2), p.10.
[39] Ofcom 2021. Children and parents: Media use and attitudes report 2021. https://www.ofcom.org.uk/__data/assets/pdf_file/0025/217825/children-and-parents-media-use-and-attitudes-report-2020-21.pdf
[40] Parentzone Scotland. Digital learning, digital life and digital work. Available at https://education.gov.scot/parentzone/my-child/digital-learning. (Accessed at
[41] Parentzone UK. Online safety hub. Available at https://parentzone.org.uk/online-safety-hub. (Accessed:16/04/2021)
[42] Prior, S. and Renaud, K., 2020. Age-appropriate password "best practice" ontologies for early educators and parents. International Journal of Child-Computer Interaction, 23, p.100169.
[43] Prior, S., & Renaud, K. 2022. The impact of financial deprivation on children's cybersecurity knowledge & abilities. Education and Information Technologies. https://doi.org/10.1007/s10639-022-10908-w
[44] Quayyum, F., Bueie, J., Cruzes, D.S., Jaccheri, L. & Vidal, J.C.T. 2021, Understanding parents' perceptions of children's cybersecurity awareness in Norway, Proceedings of the Conference on Information Technology for Social Good, pp. 236.
[45] Quayyum, F., Cruzes, D.S. and Jaccheri, L., 2021. Cybersecurity awareness for children: A systematic literature review. International Journal of Child-Computer Interaction, 30, p.100343.
[46] Rahman, N.A.A., Sairi, I., Zizi, N.A.M. and Khalid, F., 2020. The importance of cybersecurity education in school. International Journal of Information and Education Technology, 10(5), pp.378-382.
[47] Ratakonda, D.K., French, T. and Fails, J.A., 2019, June. My Name Is My Password: Understanding Children's Authentication Practices. In Proceedings of the 18th ACM International Conference on Interaction Design and Children (pp. 501-507).
[48] Reid, R. and Van Niekerk, J., 2014. Snakes and ladders for digital natives: information security education for the youth. Information Management & Computer Security.
[49] Scottish Government Education and Training National action plan on internet safety for children and young people 2017. Available at Internet safety for children and young people: national action plan - gov.scot (www.gov.scot). (Accessed:25.06.2021)
[50] Scottish Government. Cyber Resilient Scotland: Strategic Framework. 2021. Available at Cyber Resilient Scotland: strategic framework - gov.scot (www.gov.scot). (Accessed: 26.06.2021)
[51] Scottish Government. Secure and Prosperous: A Cyber Resilience Strategy for Scotland. 2015. APS Group. Available at https://www.gov.scot/binaries/content/documents/govscot/publications/strategy-plan/2015/11/safe-secure-prosperous-cyber-resilience-strategy-scotland/documents/00489206-pdf/00489206-pdf. (Accessed:03/07/2021)
[52] Snow, C.E., 2006. What counts as literacy in early childhood? in Blackwell Handbook of Early Childhood Development, Blackwell Publishing LTD, Oxford
[53] Stewart, M., Campbell, M., Renaud, K. and Prior, S., 2020, September. KidzPass: authenticating pre-literate children. In 2020 Dewald Roode Workshop on Information Systems Security Research. IFIP Working Group 8.11/11.13.
[54] ThinkUKnow. How to stay cyber secure: a short guide. Available at https://www.thinkuknow.co.uk/professionals/our-views/how-to-stay-cyber-secure-a-short-guide. (Accessed:27.07. 2021)

[55] Tirumala, S.S., Sarrafzadeh, A. and Pang, P., 2016, December. A survey on Internet usage and cybersecurity awareness in students. In *2016 14th Annual Conference on Privacy, Security and Trust (PST)* (pp. 223-228). IEEE.
[56] Utkina, O.N. and Yugova, N.L., 2020, November. The Pedagogical Technique for Teachers to Ensure Information Security of the Learning Process in the Context of the COVID-19 Pandemic. In Research Technologies of Pandemic Coronavirus Impact (RTCOV 2020) (pp. 58-62). Atlantis Press.
[57] Venter, I.M., Blignaut, R.J., Renaud, K. and Venter, M.A., 2019. Cyber security education is as essential as "the three R's". Heliyon, 5(12), p.e02855.

Appendix

Table 1
Inclusion/Exclusion Criteria

Review 1		Review 2	
1 Inclusion	Exclusion	Inclusion	Exclusion
Sources updated in 10 years	Non relevant sources	Empirical articles in cybersecurity including primary children and education	Non relevant papers and papers that only focus on cyber safety
Include reference to cybersecurity and children	Sources that only focus on cyber safety	Papers that use keywords in title, abstract or content	Duplicate publications
Scotland or UK sources		Articles 2014-2021	Review Papers
		Peer Reviewed articles/ committee reviewed	
		Articles published in English	
		Full article	
		Clearly defined research questions, methodology and conclusions	

Table 3
Grey Literature; Online Resource

Online Sources/Resources	Cybersecurity Aspects	Age Ranges	Resources
ParentZone developed with Google	Phishing, hacking, password creation	7-11years old, split at 7-9 and 9-11	https://parentzone.org.uk/be-internet-legends

Developed "Be internet legends"	(passphrase and strength) management secret keeping, safeguarding it)		Includes lesson plans, activates, stickers and posters for teaching curriculum and resources for parents. Online game Interlard for children to play with focus on cybersecurity aspects.
Nation Cyber Security Centre (NCSC) and Think U know	Phishing (looking for suspicious emails), Passwords (passphrase advice), Hacking	Age 7-11	https://www.ncsc.gov.uk/information/cybersprinters-game-and-activities Focus of the Think know site is on safety, cybersecurity aspects are largely directed to NCSC and the game cyber sprinters and activity packs for home and at school. Meets the Scottish curriculum benchmarks for cyber resilience level 2 and 3.
Young Scot	Password creation, spotting scams (Phishing), hacking and viruses	Age 11-18	https://young.scot/campaigns/national/digi-know-information Targeted for older children, provides articles, advice, quiz and sign posts to relevant resources, NCSC and stay safe online.
GLOW Scottish Government	Passwords	As per curriculum for technologies, 3-5, 5-7, 8-10, 11-13,	https://glowconnect.org.uk/password-guidance/ Advice for teachers on how to help children create strong passwords using a word grid.
Cybersquad	Passwords	4-8, 8-10, 10+	https://cybersquad.uk/resources.html Lesson plans, activities, videos, and quizzes for Scottish teachers to meet Scottish curriculum outcomes in line with cyber resilience and passwords knowledge.
National Parent Forum of Scotland	Passwords, anti-virus software	Not specified	https://www.npfs.org.uk/wp-content/uploads/edd/2020/05/NPFS_securing_your_devices_E.pdf Aimed at parents, limited advice with links to NCSC for passwords, internet matters for age guides and stay safe online. Importance of parents promoting positive online practice as this will influence children's online behaviours.
Internet Matters UK	Viruses (advise parents to tell children to be aware of pop ups and attachments carrying viruses)	0-5, 6-10, 11-13 and 14+	https://www.internetmatters.org/resources/online-safety-guide Primarily for online safety, signposts to NCSC for security.
Get Safe Online (UK Government)	Passwords, clickjacking (virus/hacking)	<5, 6-9, 10-12, 13+	https://www.getsafeonline.org/personal/article-category/safeguarding-children/ Advice based site for parents, with restrictive practice as priority through parental controls and software.

SWGfL safe, secure, online	Passwords, Phishing, Hacking, malware, and virus	Early years, 5-7, 7-11, 11-14, 14-16	https://swgfl.org.uk/security/ UK wide resource for organisations including schools, parents, and carers. Training designed for schools at key stages linked to outcomes in the framework Education for a connected world developed by UK Council for Internet safety.

Table 4

Grey Literature; Government sources

Scottish and UK Government Sources	Cybersecurity Outcomes	Age	Link to Source
Education for a Connected World framework - 2020 edition	Password knowledge, creating a strong password, scams, phishing, viruses and other malware, hacking risks and	4-7, 7-11, 11-14, 14-18	https://www.gov.uk/government/publications/education-for-a-connected-world
Benchmarks Technologies Curriculum for Excellence	Passwords, Phishing, hacking	Early level- preschool-P1 First Level P2-P4 Second Level P5-P7 Third /fourth Level S1-S3	https://education.gov.scot/improvement/documents/technologiesbenchmarksp
Safe, secure, and prosperous: a cyber	Cyber Resilience	Society wide for building cyber	https://www.gov.scot/publications/safe-secure-prosperous-cyber-resilience-strategy-scotland/

resilience strategy for Scotland		resilience with advice for embedding within the curriculum	
Internet safety for children and young people: national action plan	Cyber Resilience	Children and young people	https://www.gov.scot/publications/national-action-plan-internet-safety-children-young-people
Cyber Resilient Scotland: strategic framework	Cyber Resilience	Society wide	https://www.gov.scot/publications/strategic-framework-cyber-resilient-scotland/

Table 5

Paper research focus

Paper Type	Paper ID
Cybersecurity Knowledge and Attitudes	P3, P5, P6, P7, P9, P10, P12, P15 P18, P19, P20, P21 P22, P26
Cybersecurity Interventions for Children	P1, P2, P4, P8, P11, P13, P14, P16, P17, P23, P24, P25, P27

Figure 3

Prevalence of the perceived cognitive aspects on cybersecurity practice.

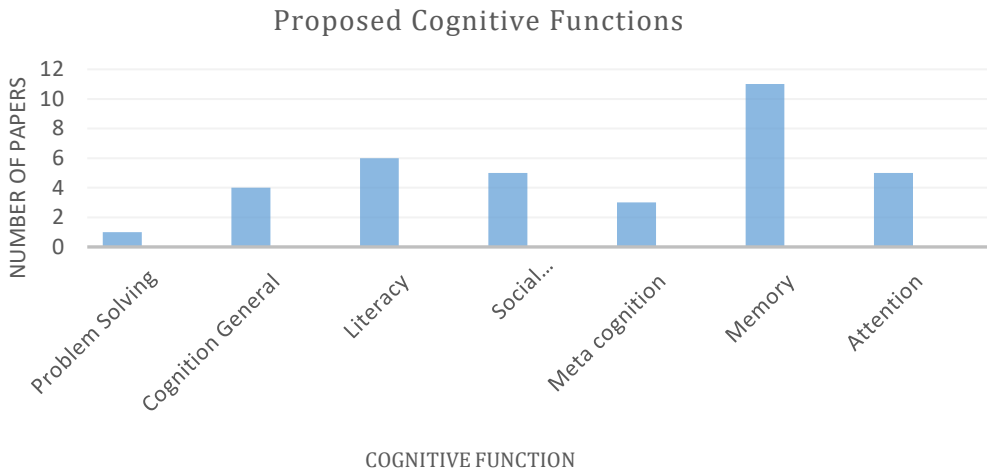


Figure 4

Cognitive functions proposed in the password management cycle

Password Problems	Cognitive Function	Paper ID
Creation	Memory	P25
	Meta Cognition	P8, P18, P19
	Attention	P8, P1
	Literacy	P7, P12, P18, P22
	Problem solving	P8
	Self-relevant	P12, P1, P2
Management	Social Learning	P24
	Secrecy	P11, P18, P26, P8
Authentication	Memory	P11, P13, P15, P18, P19, P21, P23
	Literacy	P21, P13
	Attention	P11, P2

Table 6
Papers in the Systematic Review

Paper ID	Authors	Title	Publication Source	Year	Reference number
P1	Giannakas *et al.*	A comprehensive cybersecurity learning platform for elementary education.	Information Security Journal	2019	[18]
P2	Maqsood *et al*.	An exploratory Study of Children's Online Password Behaviours	ACM Conference on Interaction Design and Children	2018	[34]
P3	Tirumala *et al.*	A survey on Internet usage and cybersecurity awareness in students.	14th Annual Conference on Privacy, Security and Trust (PST)	2016	[55]
P4	Lastdrager *et al.*	How Effective is {Anti-Phishing} Training for Children?	Thirteenth symposium on usable privacy and security	2017	[29]
P5	Lorenz *et al.*	Development of children's cyber security competencies in Estonia.	International Conference on Learning and Collaboration Technologies	2018	[32]
P6	Kumar *et al.*	'No Telling Passcodes Out Because They're Private' Understanding Children's Mental Models of Privacy and Security Online.	roceedings of the ACM on Human-Computer Interaction	2017	[25]
P7	Kumar *et al.*	Privacy and security considerations for digital technology use in elementary schools	CHI Conference on Human Factors in Computing Systems	2019	[26]
P8	Reid and Van Niekerk.	Snakes and ladders for digital natives: information security education for the youth	Information Management & Computer Security	2014	[48]
P9	Prior and Renaud.	The "three M's" counter-measures to children's risky online behaviors: mentor, mitigate and monitor.	Information & Computer Security.	2021	[42]
P10	Muir and Joinson	An exploratory study into the negotiation of cyber-security within the family home	Frontiers in psychology	2020	[36]
P11	Stewart *et al.*	KidzPass: authenticating pre-literate children.	Dewald Roode Workshop on Information Systems Security Research	2020	[53]
P12	Lamichhane and Read.	Investigating children's passwords using a game-based survey	Conference on Interaction Design and Children	2017	[28]

P13	Cole *et al.*	Click to enter: Comparing graphical and textual passwords for children.	Conference on Interaction Design and Children	2017	[14]
P14	Al Shamsi.	Effectiveness of cyber security awareness program for young children: A case study in UAE.	Int. J. Inf. Technol.	2019	[1]
P15	Kumar *et al.*	Strengthening children's privacy literacy through contextual integrity.	Media and Communication,	2020	[27]
P16	Alwanain.	How Do Children Interact with Phishing Attacks?	International Journal of Computer Science & Network Security	2021	[4]
P17	Jeong and Chiasson.	'Lime','Open Lock', and'Blocked' Children's Perception of Colors, Symbols, and Words in Cybersecurity Warnings	Conference on Human Factors in Computing Systems	2020	[22]
P18	*Choong et al.*	"Passwords protect my stuff"- a study of children's password practice.	Journal of Cybersecurity	2019	[12]
P19	Maqsood *et al.*	A day in the life of jos: a web-based game to increase children's digital literacy.	17th ACM conference on interaction design and children	2018	[34b]
P20	Macaulay *et al.*	Subjective versus objective knowledge of online safety/dangers as predictors of children's perceived online safety and attitudes towards e-safety education in the United Kingdom.	Journal of Children and Media.	2020	[33]
P21	Ratakonda *et al.*	My Name Is My Password: Understanding Children's Authentication Practices.	ACM International Conference on Interaction Design and Children	2019	[47]
P22	Choong *et al.*	Case study: exploring children's password practice and knowledge.	Workshop in Usable Security and Privacy	2019	[11]
P23	Alkhamis et al.	Kidsdoodlepass: An exploratory study of an authentication mechanism for young children.	International Symposium on Human Aspects of Information Security and Assurance	2020	[2]
P24	Chartofylaxa and Delcroix.	StoryPass–Password Rules Hidden in a Storytelling Game Activity: Steps towards Its Implementation.	Toy Research Association World Conference	2018	[9]
P25	Assal *et al.*	An exploration of graphical password authentication for children	International Journal of Child-Computer Interaction	2018	[6]
P26	Hundlani et al.	No passwords needed: The iterative design of a parent-child authentication mechanism	19th international conference on human-computer interaction	2017	[20]

			with mobile devices and services		
P27	Nicolaidou and Venizelou.	Improving children's E-safety skills through an interactive learning environment: A quasi-experimental study.	Multimodal Technologies and Interaction	2020	[38]