children

MDPI

Article

Who Is Best Placed to Support Cyber Responsibilized UK Parents?

Suzanne Prior [1] **and Karen Renaud** [1,2,3,4,*]

[1] School of Design and Informatics, Abertay University, Dundee DD1 1HG, UK; s.prior@abertay.ac.uk
[2] Department of Computer and Information Sciences, University of Strathclyde, Glasgow G1 1XQ, UK
[3] School of Computer Science, University of South Africa, Pretoria 0003, South Africa
[4] Department of Information Systems, Rhodes University, Grahamstown 6140, South Africa
* Correspondence: karen.renaud@strath.ac.uk

Abstract: The UK government responsibilizes its citizens when it comes to their cyber security, as do other countries. Governments provide excellent advice online, but do not provide any other direct support. Responsibilization is viable when: (1) risk management activities require only ubiquitous skills, (2) a failure to manage the risk does not affect others in the person's community. Cybersecurity fails on both counts. Consider that parents and carers are effectively being responsibilized to educate their children about cybersecurity, given that young children cannot be expected to consult and act upon government advice. Previous research suggests that UK parents embrace this responsibility but need help in keeping up to date with cybersecurity 'best practice'. In this paper, we consider a number of possible sources of parental advice, and conclude that support workers would be best placed to support parents in this domain. We then carried out a study to gauge the acceptability of this source of help. We find that parents would be willing to accept advice from this source, and suggest that cybersecurity academics be recruited to train support workers to ensure that they have current 'best practice' cybersecurity knowledge to impart to parents.

Keywords: parents; cybersecurity; responsibilization

Citation: Prior, S.; Renaud, K. Who Is Best Placed to Support Cyber Responsibilized UK Parents? *Children* **2023**, *10*, 1130. https://doi.org/10.3390/children10071130

Academic Editor: Paul R. Carney

Received: 10 June 2023
Revised: 23 June 2023
Accepted: 25 June 2023
Published: 29 June 2023

1. Introduction

Global citizens increasingly inhabit a digital-first world, with many services being offered online as a preferred option [1]. In 2020, UK citizens spent an average of 4 h per day online [2]. One in three Internet users were children in 2015 [3], and the Institution of Engineering and Technology (IET) reported in 2022 that children now spend more time online than in the real world [4], likely a consequence of the pandemic lockdowns [5–9].

Criminals and perverts operate in the online world to pursue their own nefarious aims. Cybercriminals target individuals, businesses and entire countries [10]. Children, too, are likely to be targeted and might actually be at greater risk than their parents [11]. As such, children should know how to keep themselves both safe and secure online [12], as they learn to do in the physical world. Safety and security are substantially different. ***Cybersafety*** is related to preventing harms resulting from online *content* (seeing adult content), *contact* (being contacted by unknown adults) and *conduct* (misbehaving online) [13]. ***Cybersecurity*** can simply be defined as "*the protection of cyber-systems against cyber-threats*" ([14], p. 29). As such, cybersafety is related to protecting the child's person and well being (including preventing cyberbullying), while cybersecurity is related to protecting the child's devices and information.

Parents routinely teach their children how to keep themselves safe in the physical world [15]. Interestingly, Statista published data which demonstrates that UK parents are also the primary source of ***cybersafety*** information for their children throughout their childhood [16]. This study found that 91% of children aged 12–15 stated that their parents were a source of cybersafety-related information. Contrast this with the percentage who

stated that they received cybersafety information from their friends, which stood at only 14%. Teachers were the second most common source of information, but still only accounted for 66–73% of children. Moreover, Smahel et al. [17] reported that parents were the main source of online-related support for children and young people. There is evidence that parental mediation can indeed support young learners in managing online risk [18].

In this paper, we consider how children can be taught about cybersecurity, and do not address cybersafety, while not denying its importance in this space. Now, consider that UK citizens, as with other neo-liberalised nations, are responsibilized to take care of their own cybersecurity [19]. A subset of citizens are parents, and they, too, are responsibilized not only to take care of their own cybersecurity, but also the cybersecurity of their children [20,21].

Previous research found that parents were happy to accept the responsibility to educate their children about cybersecurity [22,23]. However, the researchers also found that UK parents' cybersecurity knowledge was often out of date. This points to the need for UK parents to be supported and empowered if they are to be held responsible for their children's cybersecurity. It might seem obvious that the government, who is responsibilizing the parents, ought to ensure that parents are able to embrace and fulfil this responsibility. However, trust in the UK government is currently very low (with only 35% of the UK population trusting the UK government [24]). This low percentage has been confirmed by the 2023 Edelman Trust Barometer [25].

In essence, we now have a situation where parents need help to bring their cyber knowledge up to date, but they also do not trust the very entity who is able to provide them with this cybersecurity assistance and advice [26]. In this paper, we report on an alternative way to empower UK parents in this respect, to help them to act upon and fulfil their cyber responsibilities towards their children. We carried out a Q-methodology study to gauge which source of correct and trustworthy advice would be deemed acceptable to UK parents.

Section 2 reviews the related research. Section 3 proposes a way to provide UK parents with more support in educating their children about cybersecurity. Section 3.1 then outlines the study we carried out to determine the acceptability of our proposed intervention to UK parents. Section 4 discusses the results and considers the research implications of our findings and mentions the limitations of this investigation. Section 5 concludes.

2. Related Work

2.1. Responsibilization

Responsibilization theory [27] revolves around the concept of assigning responsibility to individuals and influencing them to embrace those responsibilities. This theory emphasises the transformation of individuals into self-reflexive and self-directed agents, capable of taking charge of various aspects of their lives without relying heavily on government support. The aim of responsibilization is to promote self-reliance and reduce the burden on government services. According to Pellandini-Simányi and Conte [28], responsibilization encompasses both the assignment of responsibility to citizens and the influence of social and cultural factors that persuade individuals to accept and fulfill those responsibilities. The theory aims to create a society of empowered individuals who actively participate in decision-making processes and take ownership of their actions. Effective implementation of responsibilization theory requires two key factors.

Firstly, citizens must be willing and able to carry out their cyber-related responsibilities. It is crucial for them to possess the necessary competence to embrace their responsibilities fully. This involves equipping individuals with the knowledge, skills, and resources required to fulfil their assigned roles. Secondly, it is crucial to ensure that the failure of individuals to act upon their responsibilities does not harm others. This aspect highlights the importance of balancing individual autonomy and collective well-being within the framework of responsibilization. By examining these dimensions, responsibilization

theory provides insights into how governments and societies can promote a culture of self-sufficiency while maintaining social cohesion and responsibility.

Given the lack of cybersecurity knowledge demonstrated by UK parents [22,29], it is unlikely that the first requirement can be met. UK parents' inability to fulfil their state-assigned and willingly accepted responsibility to educate their children about cybersecurity is likely to result in the unwitting dissemination of incorrect and outdated advice. This, in turn, will result in the widening of the cybersecurity divide [30]. Parents might not be aware of this situation, and even if they are aware, might well choose not to confront it or actively seek to improve their cybersecurity knowledge. If they realise that they are in this quandary, they might well consult external support or resources to get advice.

2.2. Children's Cybersecurity Education

There is widespread acknowledgement that it is important to educate children about cybersecurity [31–37]. Throughout the UK, cybersecurity is included in the curriculum for children throughout their time at school. However, the extent to which it is covered varies by individual nation [38]. In addition, no curriculum in England fully covers the basic topics defined by the UK government as being necessary for good personal cybersecurity [39].

Some authors have commented on the fact that while awareness is high, or improved by lessons, this does not necessarily convert to secure behaviours [40,41]. This suggests that efforts at school need to be augmented at home, so that educational efforts are reinforced by parents, as is common for other educational domains [42].

Quayyum [43] argues for the significant role parents play in in cybersecurity education. Therefore, it falls to UK parents to educate their children. Previous research has shown that UK parents embrace this responsibility [22]. They might well consider this to be part of the activities they carry out to consider themselves to be 'good parents'. The danger in relying upon parents to fulfil this role without external support is that their level of knowledge cannot be guaranteed to be sufficient enough to perform this task. Indeed, recent research has suggested it is poor [22], in line with cybersecurity knowledge across the UK population [44].

A variety of cybersecurity resources are freely available [45]. However, there are issues with many of these, in particular books, which have often been found to contain out-of-date or incorrect guidance [46]. In addition, even when children are able to engage independently with the many online resources [38], they still require input from adults to explain how to apply the principles. That being so, we cannot feasibly expect children to teach themselves the correct principles.

2.3. Empowering UK Parents with Cyber Advice

While it is crucial that efforts continue to be made in addressing and improving children's knowledge, similar efforts must be invested into improving parents' knowledge, given their responsibility for teaching their children about cybersecurity best practice.

At present, it would appear that parents do not possess sufficient up-to-date knowledge to be responsible for managing the cybersecurity education of their children, nor do they consult the most reliable sources to obtain such knowledge [22]. Recent government campaigns have had little impact (e.g., using passphrases instead of complex passwords) [47].

Even so, parents do demonstrate a willingness to accept advice from educational authorities and cybersecurity academics. This offers an opportunity for intervening to provide more support to responsibilized UK parents. Advice sources can be judged on two dimensions: (1) whether they provide correct advice, and (2) whether they are trusted [48,49]. The first is crucial because if someone gets the wrong or outdated cybersecurity advice, at some point they are likely to be confronted by the correct advice. When that happens, they have to unlearn the previous information, which is challenging to do [50,51]. The second is equally important because trust levels influence behaviours [52]. Let us now consider each of the possible sources of advice as shown in Figure 1.

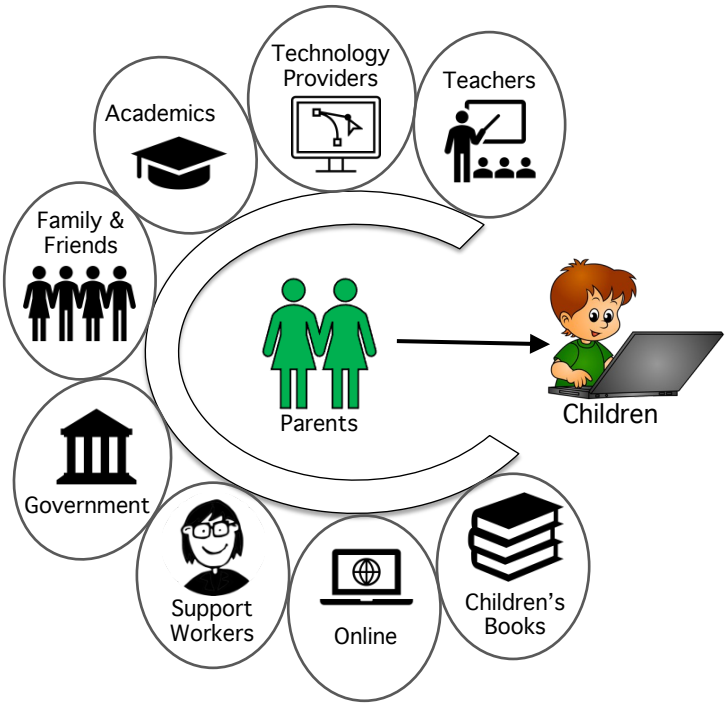

Figure 1. Possible Sources of Cyber Advice for Parents.

2.3.1. Government as Source

While responsibilization is a government strategy, and embraced by parents, it is clearly a challenge for governments to support parents in this respect due to low trust levels [24–26]. The respondents in [22] were unwilling to trust cybersecurity-related advice issued by the UK government, possibly due to recent events in the UK [53,54].

2.3.2. Teachers as Source

Parents were willing to accept advice from education professionals and cybersecurity academics [22]. Moreover, Ipsos MORI surveys revealed that teachers remained a trusted profession in the UK [55,56]. However, teachers themselves also appear to struggle to keep up with the latest cybersecurity knowledge [12,57,58]. Moreover, teachers' workloads are such that it is unlikely they have the bandwidth to keep up with the latest cybersecurity developments or to provide support to parents [59]. Cybersecurity education is indeed included in primary school curricula, but the topics and approaches to teaching these vary, depending on the educational authority [38]. Moreover, childhood deprivation has a deleterious impact on how well children learn these principles at school [30].

2.3.3. Family and Friends as Source

Muir and Joinson [23] reported that many people relied on family and friends for cybersecurity advice. In another study, it emerged that a third of parents sought cybersecurity advice from their own friends and family [22]. However, given the general lack of cybersecurity knowledge across the UK population [22], this might well lead to incorrect advice spreading throughout the community, which may further widen the cyber divide discussed in [30].

2.3.4. Children's Books as Source

The UK has societies that encourage the buying of books for children [60]. Queen Camilla and the Princess of Wales promote the reading of books to children [61]. However, children's books do not provide up-to-date cyber security principles [46]. This is unsurprising since the advice responds to dynamic and ever-changing cyber threats, and books, in print format, cannot possibly change as quickly.

2.3.5. Cybersecurity Academics as Source

UK academics are generally trusted by the public [62]. The pandemic might easily have dented this trust [63] but luckily, the British Academy's recent study found that academics are still widely trusted [64]. Cybersecurity academics work with psychologists and computer scientists to understand how to deliver cybersecurity guidance to the public. Cybersecurity academics can also be expected to give correct advice, given that this is their primary focus.

However, research related to empowering parents is still rather sparse. For example, Al-Naser et al. [65] revealed a lack of information for children aged six years or below, when it comes to smart device cybersecurity. Prior and Renaud [45] developed an age-appropriate approach to educating children about password best-practice, which was intended to help both teachers and parents, and to fill the knowledge gap that exists with respect to password 'best practice'.

2.3.6. Online Advice as Source

Google determined, in a 2019 study, that people tended to trust their search results [66]. Moreover, [22] found that people preferred to rely on results returned by a search engine in terms of finding advice on cybersecurity matters, as opposed to other sources of information. However, there is a great deal of variety in offered advice and Renaud and Prior [12] found that many online sources provided incorrect and out-of-date advice, unlike the advice provided by the UK's National Cybersecurity Centre [67].

For example, at present the BBC (the UK public broadcasting service) website for children (CBBC) [68] requires the use of lower case, upper case, digit, special character (LUDS) when creating a password. This is outdated and no longer 'best practice' [67].

The CBBC site also asks the user to set a username. While it does not require this to be the child's actual name, it also does not disallow this. Furthermore, if the child forgets their password, it cannot be reset and a new account must be created. This may encourage the use of very weak passwords.

2.3.7. Technology Providers as Source

There is certainly an opportunity for technology providers and companies to be proactive in protecting children's cybersecurity. This should be routine throughout all reputable online services, which is not the case at present.

The UK Government is working on 'Secure by Design' legislation called Product Security and Telecommunications Infrastructure (PSTI) Act. This, if realised, could give technology providers a role to play in terms of more secure architectures for computer hardware. However, the idea that they could play a role in providing advice to UK citizens does not appear to have been envisaged. At the moment, this group does not seem to be widely consulted for cybersecurity advice [22].

2.3.8. Support Workers as Source

Support workers or family liaison workers enjoy a great deal of trust in the UK [69]. These are are professionals who provide support, guidance, and assistance to families in challenging circumstances or during significant events. These individuals are typically employed within various sectors, such as law enforcement agencies, social services, or educational institutions, to act as a vital link between families and the relevant organisations or authorities.

Support workers facilitate information exchange, coordinate services, and ensure that families have access to the necessary support networks and play a crucial role in promoting collaboration and cooperation between families and the organisations.

This has the potential to bridge the cybersecurity knowledge gap. Within UK schools, these members of staff work primarily with 'at risk' families, supporting them in engaging with the schools, with financial challenges or supporting their children through educational difficulties [70]. They also work with the school community as a whole.

However, they do not necessarily have current cybersecurity knowledge since their training is usually health-related. This study set out to identify the most acceptable source of information. The next step would be to explore the logistics of delivering cybersecurity advice in this way—support workers are often overloaded [71]. Unless this issue is addressed, they will not be in a position to take on this additional duty.

2.4. In Summary

We have reviewed the literature and considered all usual sources of cyber advice and found issues with all of them. However, it is worth noting that the UK's National Cyber Security Strategy [72] includes the following statement: "*Civil society organisations and community groups also play a major role supporting people to understand and protect themselves from cyber risks. Many charities, for example, provide targeted support, advice and awareness-raising to vulnerable groups*". This suggests that we should go beyond traditional sources in empowering UK parents. Table 1 summarises the discussion, showing the trustworthiness of the different cybersecurity advice sources, based on Redmiles et al.'s [49] findings that '*participants evaluated digital-security advice based on the trustworthiness of the advice source*'.

Table 1. Summary of Advice Source Advice Provision Dimensions. (✔: Correct Advice, ✗: Incorrect Advice, ?: Currently Unknown, ≈: some correct/some incorrect).

Acronym	Advice Source	Provides Correct Advice	Trustworthiness
G	UK Government	✔	✗ (Mistrusted)
T	Teachers	≈	✔ (Trusted)
FF	Family & Friends	≈	✔ (Trusted)
O	Online	✗	✔ (Trusted)
A	Cybersecurity Academics	✔	✔ (Trusted)
BK	Children's Books	✗	✔ (Trusted)
SW	Support Workers	?	✔ (Trusted)

3. Proposal

It is crucial that parents' knowledge is improved, especially parents who are at the greatest risk of exclusion from traditional educational sources i.e., those with lower levels of education who have less or incorrect cybersecurity knowledge. Their children are likely also to have have lower levels of knowledge, given the findings of other studies.

One group of professionals already working with these families are family support or liaison workers. These professionals already take on a variety of roles, and, as such, they would also require support in order to be able to include cybersecurity as part of the guidance they offer to families. It is important to acknowledge that this should be considered a long-term endeavour. The challenges of achieving this include:

(1) Ensuring that there are enough support workers, where the UK currently has a shortage (https://teach-now.co.uk/tackling-the-teaching-assistant-shortage/, accessed on 24 June 2023). Moreover, recruiting those who would be willing to undertake their current duties as well as their new cybersecurity advice-giving duties;

(2) Linked to (1), recruiting enough new trainees to ensure that the number of support workers stay at a constant level;

(3) Obtaining funding from government for this endeavour [73], especially post-pandemic when it is more likely for funding to be cut [74];

(4) Cybersecurity would have to be added to a support worker training framework such as the UK's National Health Service's AHP Support Worker Competency, Education and Career Development Framework (https://www.hee.nhs.uk/our-work/allied-health-professions/enable-workforce/developing-role-ahp-support-workers/ahp-support-worke

r-competency-education-career-development, accessed on 24 June 2023). It takes time for this kind of change to be approved at all levels;

(5) These workers are poorly paid at present [73], and unless this is remedied, it is unlikely that they would be willing to take on extra duties;

(6) Managing parental expectations is crucial [73]. It would be all too easy for them to be asked, by parents and the school, to fix computers or remove malware. Moreover, the school might want them to teach the children about cyber, which would make their role unsustainable. Their role would have to be clearly defined in their job statement to protect them. It would have to be made clear that their role is **only** to provide correct and trustworthy advice;

(7) Finally, looking to the future, it is likely that there would be calls for certifications of these workers in their cyber advice role. If extra training could help to address the current lack of career progression opportunities and the current lack of respect for these workers [73], this could be a positive, but only if this is something they would want to do.

Academics working in cybersecurity could work directly with these professionals, training them in the most up-to-date cybersecurity knowledge. They would then be able to communicate this to the families they assist as part of their work in engendering good education and health practices (see Figure 2).

Resources for families should be designed considering a variety of ethnic groups and languages. By working with various groups and language specialists, academics could help to produce resources for use for all parents. This would require further investment into these roles by government and willingness from academics to provide this form of support.

These resources could be provided free of charge to parents and would require only small periods of time to read [75]. The question of how this would be funded is clearly still an open one. However, the current situation, with increasing cyber attacks occurring [76], and children being poorly protected when online, cannot continue. Funding support workers would be a cost-effective way of addressing the situation.

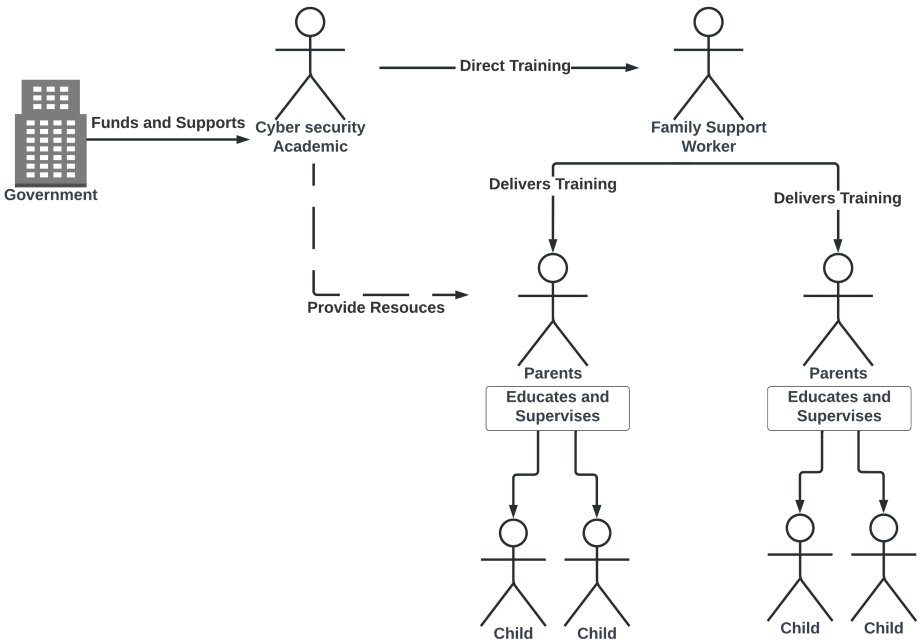

Figure 2. Proposed Support for Parent responsibilization.

3.1. Gauging Acceptability of Proposal

Given that we are proposing an intervention that is, as yet, unvalidated, we carried out a study that assesses subjectivity to help us understand people's thinking with respect to the acceptability of this source of assistance. We deployed Q-methodology to carry out this final study. This method was introduced by Stephenson [77]. It specifically supports the

systematic study of subjectivity. Q-methodology measures beliefs *as cultural phenomena*. and helps to reveal beliefs shared by groups of individuals. The findings from a Q-methodology analysis helps to assess the *nature* of subjectivity: '***what is the nature*** *of different groups' thinking?'*, as opposed to '***how*** *are people thinking on the topic?'*. This methodology does not require large numbers of participants [78].

Q-methodology reveals correlations between subjects across a sample of variables: the "Q-set". It is composed of 'Q-statements'. A factor analysis is then used to isolate the most influential "factors", which reflect cultural ways of thinking. The method's strength is that it applies sophisticated factor analysis to support a qualitative analysis. The qualitative part of the analysis uses free-text responses where respondents are asked to explain why they agree or disagree with particular statements. This methodology does not seek to confirm or deny specific hypotheses; it aims to provide a sense of '*potentially complex and socially contested*' issues [79]. Figure 3 depicts the steps involved in a Q-sort.

Figure 3. Q-Sorting Process.

3.1.1. Q Statements

Q-Statements for this study were derived from the results reported by [22] in response to questions relating to sources of help and the respondents' free text responses. These were confirmed from the cybersecurity-related research literature.

Participants sort Q-Statements into a fixed quasi-normal distribution, ranging from −4 (disagree) to +4 (agree). They can amend and confirm their rankings and then provide open-ended comments for the most agreed-with (ranked +4) and most disagreed-with (ranked −4) statements (Table 2). This helps us, as researchers, to gain insights into the range of opinions about our topic of investigation [78].

Table 2. Q Statements (Acronyms from Table 1) G = Gov, P = Parents; T = Teachers; A = Academics; SW = Support Workers; TP = Technology Providers; C = Children.

#	Statement	Entity
1.	I know where to get reliable cybersecurity advice [80]	P
2.	I think the UK government provides helpful cybersecurity advice to parents (testing source)	G
3.	I can act upon the cybersecurity advice I am given by the UK government [81]	G
4.	My child's teacher is well informed about cybersecurity [46]	T
5.	Cybersecurity academics are aware of the latest cybersecurity precautions (testing source)	A
6.	I would be happy to accept cybersecurity advice from family support workers/family liaison officers [82]	SW
7.	The UK government provides helpful cybersecurity advice [22]	G
8.	I would be happy to accept cybersecurity advice from cybersecurity academics (testing source)	A
9.	When I receive cybersecurity advice from my child's school, I act on it (testing source)	S
10.	I feel confident in educating my child(ren) about cybersecurity precautions and good practice [75]	P
11.	I am uncertain about different cybersecurity practices [83]	P
12.	I am happy with how technology providers currently assure my child's cybersecurity [84]	P
13.	I think technology providers could be doing more to provide better cyber security controls for children [84]	TP

Table 2. *Cont.*

#	Statement	Entity
14.	The UK government needs to enforce higher cybersecurity standards from technology providers [84]	G, TP
15.	The UK government should not meddle with the way technology providers deal assure cybersecurity	G
16.	There are plenty of cybersecurity resources for parents, schools do not need to get involved [85,86]	P
17.	I would blame myself if my child's cybersecurity was compromised [87]	P
18.	I think children need to take responsibility for their online cyber security actions (testing responsibility)	C
19.	I am not an expert, it is up to my child's educators to teach them about cybersecurity [32]	T
20.	The UK government should take ultimate responsibility for protecting my child's cybersecurity (testing responsibility)	G
21.	Hackers are not targeting children online so they don't need to learn about cybersecurity until they are adults [88]	
22.	Parents should figure out how to teach their children about cybersecurity without help from anyone else (testing responsibility)	P
23.	I am confident in my ability to teach my children about cybersecurity [89]	P
24.	I do not have confidence in the UK government's ability to help me teach my child about cybersecurity [90]	G
25.	Parents should be responsible for teaching their children about cybersecurity [22]	P

3.1.2. Recruiting

UK-based parents with children aged less than 18 years of age were recruited via the Prolific platform. Ethical approval was granted by the second author's institution's ethical review board. Measures to obtain informed consent and to ensure anonymity of participants' responses were implemented.

Forty participants were recruited on the Prolific platform. This is consistent with recommended participant group sizes in Q-methodology [79]. 15 of the participants were female, 19 were male and 6 preferred not to specify their gender. Ages ranged from 25 to 74 years of age. Based on the pilot study timings, we paid participants £2 for 10 min of labour, exceeding the UK minimum wage. Participants did not provide any personal data, ensuring that participation was anonymous.

3.2. Analysis & Findings

We extracted factors using the principal component extraction technique and applied a varimax procedure for factor rotation. Factors with an eigenvalue in excess of 2.00, and having at least two significantly loading participants, were selected for interpretation (as recommended by [79]) (Figure A1 in the Appendix A).

Before we discuss each of the factors, we need to point out that all respondents most strongly disagreed with Statement 21: "*Hackers are not targeting children online so they don't need to learn about cybersecurity until they are adults*". This means that all parents are well aware of the risks to themselves and their children online. The final Q-Sorts are shown in Figures A2–A6 in the Appendix A).

Factor 1: The Government should enforce higher cybersecurity standards and they would accept cybersecurity-related advice.

This factor explained 40% of the variance, with an eigenvalue of 15.83. 15 Participants (8M, 4F, 3 preferred not to say) belonged to this group, aged 25 to 74 (average age 43.6). One respondent said: "*They need to make sure we are safe in this technology used*" and "*i think they shoud care more about it, as no one is safe at the moment*". However, they, themselves, struggled with cybersecurity knowledge, because they were looking for advice: agreement

with statements 6, 8, and 9. One respondent said: "*Because I don't have a lot of confidence in my knowledge of cyber security I trust the school and their advice and know they are thing me age appropriate cyber security. This is a definite agree that I would follow their advice*".

Factor 2: Embrace the idea of taking personal responsibility, and would accept advice from various sources.

This factor explained 11% of the variance. Seven participants (4M, 2F, 1 preferred not to say) loaded to this factor, aged from 28 to 54 (average 41.2). This group embrace responsibility: "*i think they [think] it is the patents [sic] responsibility to teach their kids how to be safe*", and "*I teach my children how to take responsibility for all their own actions and support them in doing so. I never make my children solely responsible*". They also agreed with statements related to accepting advice from academics and family support workers. They do not believe that government has a role to play in this respect: " *It's not up to the government to take responsibility. The internet is a worldwide channel. People will always find a way round*", but they do believe that government-provided advice is helpful (agreeing with Statement 7).

Factor 3: Do not trust the government to keep their children safe, and would accept advice from various other sources:

This factor explained 8% of the variance. Eight participants (3M, 4F, 1 preferred not to say) loaded to this factor, aged from 31 to 49 (average 37). One respondent said: "*Because I don't have any confidence in them for anything. Especially with everything else that is happening*", but agreed with statements 6 and 8, indicating a willingness to accept and act upon cybersecurity advice, but not from the government (disagreeing with statement 7). It is safe to conclude that this group would like to take care of their own children's cybersecurity educational needs, but do not want the government to be involved.

Factor 4: Express a need for more cybersecurity advice and feel confident in acting upon advice:

This factor explained 6% of the variance. Eight participants (3M, 5F) loaded to this factor, aged from 36 to 69 (average 41.2). This group also agree with statements 6, 8 and 9, these being most strongly agreed with. They have confidence to act upon this advice: " *I am very computer and cyber savvy I use technology all the time so i'm quite confiident [sic]*". They would not blame themselves if their child was hacked (Statement 17).

Factor 5: Believe that the government ought to require technology providers to do more, and are confident in their own ability to find cybersecurity guidance.

This factor explained 5% of the variance. Two participants (1M, 1 preferred not to say) loaded to this factor, aged 35 and 62. This group does not have confidence in the government's ability to teach children about cybersecurity best practice: "*Because I don't have any confidence in them for anything. Especially with everything else that is happening*". They had confidence in their own abilities, disagreeing with: " *I do not know that much about it myself to help*" and agreeing with statements 10 and 23.

4. Discussion and Reflection

The findings from our study confirm that participating UK parents embraced being responsibilized to educate their children about cybersecurity, probably a logical extension of all their other parental duties. As such, they accept this responsibilization, and do their best to find information to meet its demands.

It is thus unsurprising that three of the five factors strongly suggest that they could blame themselves if their children were hacked (Statement 17). In the free-text comments, one said: "*i feel children should mainly be taught cybersecurity by parents*". Another said: "*It's my responsibility upon this to keep my children safe*". This confirms that UK parents are seeking more advice and guidance from external sources. The factors also pointed to a lack of trust in the UK government to provide this advice and guidance. This showed that

parents were least likely to accept advice from the UK government. This validates the need to find a different way to provide them with the advice they need, as proposed by our intervention (Figure 2).

However, it is important to ensure that these support workers are given the knowledge they need to fulfil this new role, and it seems that cybersecurity academics are best placed to train them. Academics are trusted by parents—four of the five factors showing that people agreed that academics would have the most up to date information. Knowing that they are providing the information might increase the trustworthiness of the support workers in providing support and advice to parents.

The study also revealed that parents feel the government should force companies and technology providers to take their cybersecurity and cybersafety responsibilities more seriously. At the time of the study this was an issue in the UK press regarding the proposed Online Safety Bill [91]. This indicates that parents are willing to have some of the burden of responsibilization lifted from them.

4.1. Research Implications

Firstly, it would be interesting to understand why it is that parents so willingly accept their responsibilization to educate their children about cybersecurity, given the relative complexity of the risk management activities in this domain. They willingly leave their children's education with respect to reading, writing, arithmetic and other areas to schools. They take their children to specialists to teach them to swim, play musical instruments and do gymnastics. Is it because cybersecurity is seen as an extension of cybersafety? Is it because they have become used to doing it? It would be interesting to explore this in greater depth by running focus groups with parents.

Secondly, the devil being in the details, we would have to flesh out the intervention to see exactly what would be required to implement it. It might be that the school liaison officers would be too intimidated by cybersecurity themselves. The government might not have the resources to fund this, especially given the current era of cost-of-living challenges [92]. Hence, fleshing out the intervention very carefully and coming up with funding models would be essential to determine its feasibility.

Thirdly, we need to understand what other barriers exist that may prevent parents being willing or able to take this advice on board.

4.2. Limitations

Our study was carried out while the UK's Prime Minister election was ongoing, in the aftermath of politician misbehaviour which is bound to affect trust in government [93]. It is likely that these events shook confidence in the UK government's competence, integrity and benevolence, all of which are essential in fostering trust in governments [94]. Our studies did not examine ethnicity. Work in other areas of responsibilization of education (for example during the lockdowns of 2020 and 2021) demonstrated that those from ethnic minorities were affected more negatively than others [95].

We carried out this study to identify the most acceptable and trustworthy source of correct cybersecurity advice, from parents' perspective. The sample was relatively small, although comparable with other Q-methodology studies, and indeed in line with expert recommendations [77]. Even so, we would have to follow up with a large scale survey of the UK population in order to confirm our findings. Admittedly, as acknowledged in this paper, everything hinges on the UK government or charities being willing to provide funds for more support workers to fulfil this additional role of cyber adviser.

5. Conclusions and Future Work

The burden for citizens of managing their own cybersecurity practices and protections has been further placed on parents when it comes to handling their children's cybersecurity education. However, traditional sources of advice and support (books, online sources, etc.) are unreliable, or not trusted (government). Hence, we have suggested a mechanism for

providing parents with the support they need, which is: (1) well informed because they work with cyber security academics, and (2) already trusted by parents.

Our study confirmed that our proposed intervention for providing cybersecurity-related advice and support is likely to be accepted by UK parents, although we would have to carry out a more extensive study to confirm this. The benefit is likely to be well informed and confident parents in the cyber realm, and less vulnerable children across the United Kingdom.

Author Contributions: Conceptualization, S.P. and K.R.; methodology, S.P. and K.R.; formal analysis, S.P. and K.R.; data curation, K.R.; writing—original draft preparation, S.P.; writing—review and editing, S.P. and K.R.; visualization, K.R.; funding acquisition, S.P. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: The study was conducted in accordance with the Declaration of Helsinki, and approved by the Institutional Review Board (or Ethics Committee) of Abertay University (protocol code EMS5449 28.01.22, Approval Date: 27 October 2022) for studies involving humans.

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Data Availability Statement: Dataset available from https://rke.abertay.ac.uk/en/datasets/ (accessed on 24 June 2023).

Acknowledgments: We thank the participants for their time and considered answers. We thank Karl van der Schyff for his help with the design of the study. We also thank Natalie Coull and Gareth Renaud for their feedback on an earlier draft of this paper.

Conflicts of Interest: The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

Appendix A

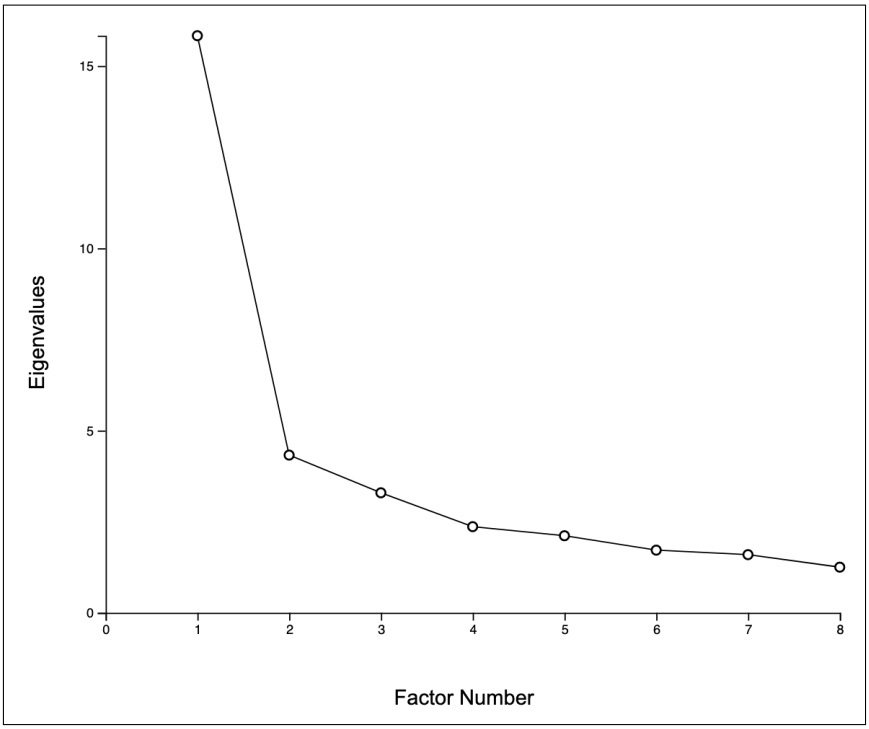

Figure A1. Scree Plot.

Factor Statement Loadings: Please note that due to space constraints, in these Figures cybersecurity is reflected as CS, and statements are sometimes truncated (...). Full statements are provided in Table 2.

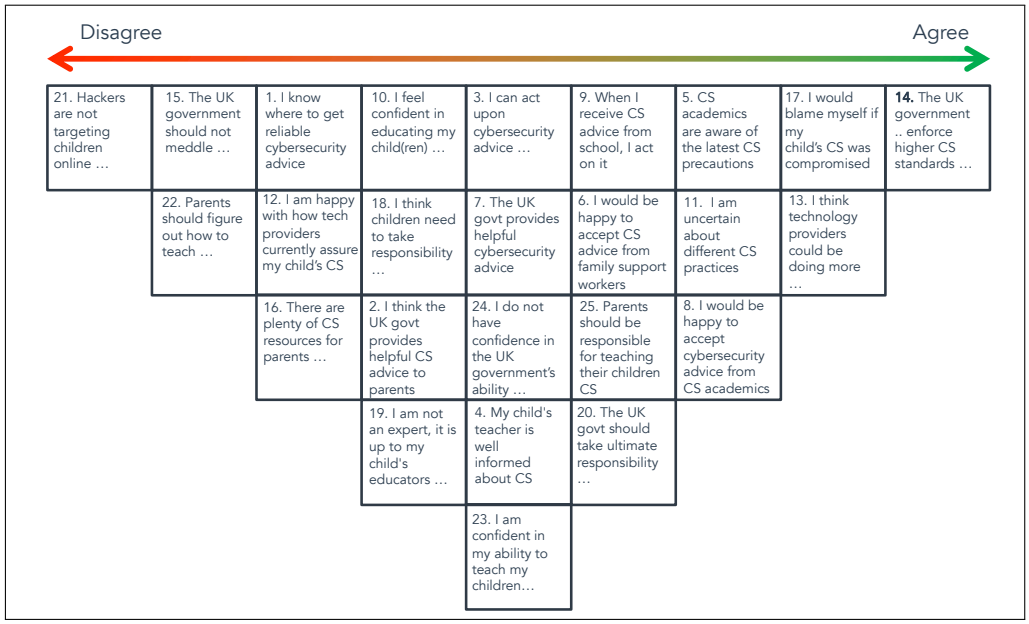

Figure A2. Factor 1 Q-Sort.

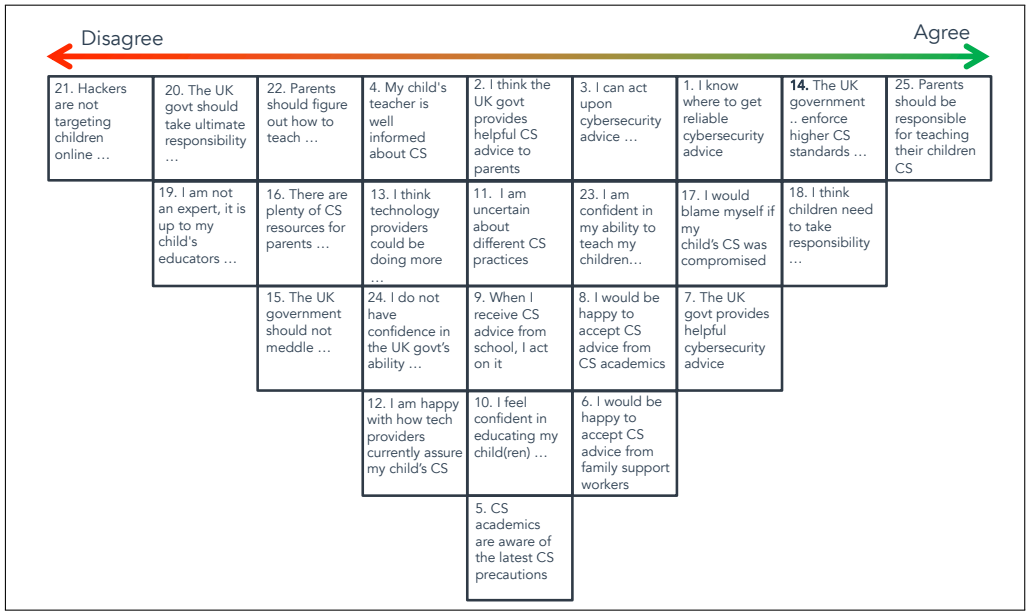

Figure A3. Factor 2 Q-Sort.

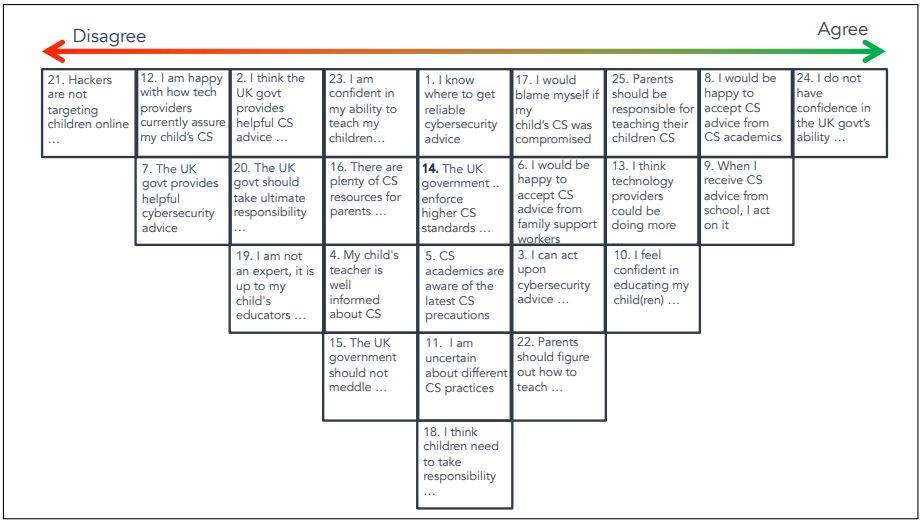

Figure A4. Factor 3 Q-Sort.

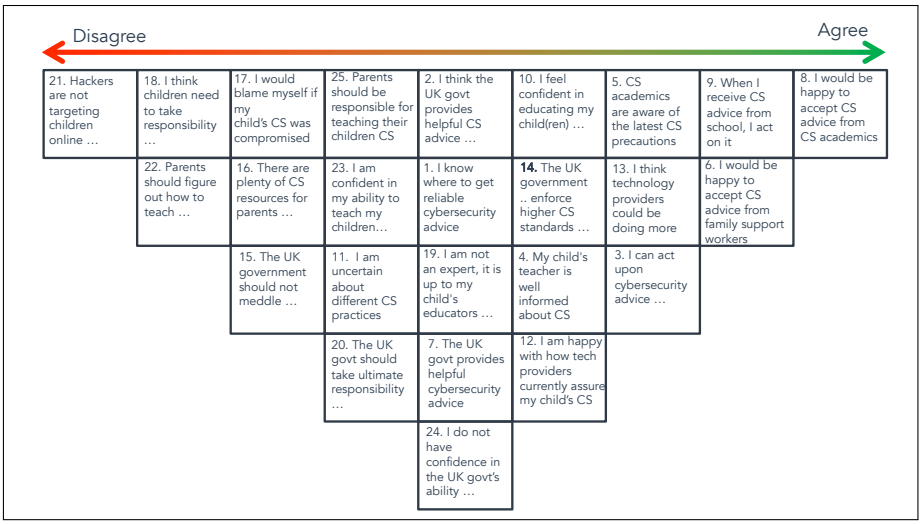

Figure A5. Factor 4 Q-Sort.

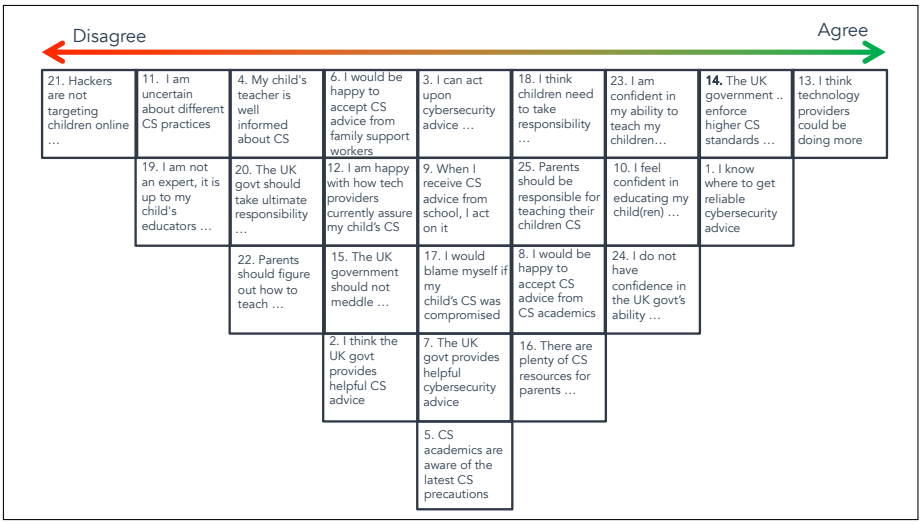

Figure A6. Factor 5 Q-Sort.

References

1. Pérez-Morote, R.; Pontones-Rosa, C.; Núñez-Chicharro, M. The effects of e-government evaluation, trust and the digital divide in the levels of e-government use in European countries. *Technol. Forecast. Soc. Chang.* **2020**, *154*, 119973. [CrossRef]
2. Ofcom. UK's Internet Use Surges to Record Levels. 2020. Available online: https://www.ofcom.org.uk/about-ofcom/latest/media/media-releases/2020/uk-internet-use-surges (accessed on 1 September 2022).
3. Livingstone, S.; Carr, J.; Byrne, J. *One in Three: Internet Governance and Children's Rights*; UNICEF, Office of Research-Innocenti: Florence, Italy, 2016.
4. The Institution of Engineering and Technology. Engineering Kids' Futures. 2022. Available online: https://www.theiet.org/media/campaigns/engineering-kids-futures/ (accessed on 3 May 2023).
5. Office for National Statistics. Children's Online Behaviour in England and Wales: Year Ending March 2020. 2020. Available online: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/childrensonlinebehaviourinenglandandwales/yearendingmarch2020 (accessed on 1 September 2022).
6. Fischer, S. Kids' Daily Screen Time Surges during Coronavirus. 2020. Available online: https://www.axios.com/kids-screen-time-coronavirus-562073f6-0638-47f2-8ea3-4f8781d6b31b.html (accessed on 20 June 2020).
7. Torluemke, J.; Kim, C. NortonLifeLock Study: Majority of Parents Say Their Kids' Screen Time Has Skyrocketed during the COVID-19 Pandemic. 2020. Available online: https://investor.nortonlifelock.com/About/Investors/press-releases/press-release-details/2020/NortonLifeLock-Study-Majority-of-Parents-Say-Their-Kids-Screen-Time-Has-Skyrocketed-During-the-COVID-19-Pandemic/default.aspx (accessed on 20 June 2020).
8. Peek, N.; Sujan, M.; Scott, P. Digital health and care in pandemic times: impact of COVID-19. *BMJ Health Care Inform.* **2020**, *27*, e100166. [CrossRef] [PubMed]
9. Walsh, B.; Rana, H. Continuity of academic library services during the pandemic the University of Toronto libraries' response. *J. Sch. Publ.* **2020**, *51*, 237–245. [CrossRef]
10. Attatfa, A.; Renaud, K.; De Paoli, S. Cyber diplomacy: A systematic literature review. *Procedia Comput. Sci.* **2020**, *176*, 60–69. [CrossRef] [PubMed]
11. Hazlegreaves, S. Children Are Becoming More Vulnerable to Cybercriminals as IOT Device Use Explodes. 2019. Available online: https://www.openaccessgovernment.org/children-vulnerable-to-cybercriminals/72665/ (accessed on 1 September 2022).
12. Renaud, K.; Prior, S. The "three M's" counter-measures to children's risky online behaviors: mentor, mitigate and monitor. *Inf. Comput. Secur.* **2021**, *29*, 526–557. [CrossRef]
13. Byron, T. Safer Children in a Digital World: The Report of the Byron Review: Be Safe, Be Aware, Have Fun. 2008. Available online: https://dera.ioe.ac.uk/id/eprint/7332/ (accessed on 1 May 2023).
14. Refsdal, A.; Solhaug, B.; Stølen, K. Cybersecurity. In *Cyber-Risk Management*; Springer: Oslo, Norway, 2015; pp. 29–32. [CrossRef]
15. Wurtele, S.K.; Gillispie, E.I.; Currier, L.L.; Franklin, C.F. A comparison of teachers vs. parents as instructors of a personal safety program for preschoolers. *Child Abus. Negl.* **1992**, *16*, 127–137. [CrossRef]
16. Statista. Internet Usage in the United Kingdom (UK)—Statistics & Facts. 2022. Available online: https://www.statista.com/topics/3246/internet-usage-in-the-uk/ (accessed on 1 August 2022).
17. Smahel, D.; MacHackova, H.; Mascheroni, G.; Dedkova, L.; Staksrud, E.; Olafsson, K.; Livingstone, S.; Hasebrink, U. *EU Kids Online 2020: Survey Results from 19 Countries*; London School of Economics and Political Science: London, UK, 2020. [CrossRef]
18. Purnama, S.; Ulfah, M.; Machali, I.; Wibowo, A.; Narmaditya, B.S. Does digital literacy influence students' online risk? Evidence from COVID-19. *Heliyon* **2021**, *7*, e07406. [CrossRef]
19. Renaud, K.; Orgeron, C.; Warkentin, M.; French, P.E. Cyber security responsibilization: an evaluation of the intervention approaches adopted by the Five Eyes countries and China. *Public Adm. Rev.* **2020**, *80*, 577–589. .. [CrossRef]
20. Behar, N. Good Cybersecurity Starts at Home. Ph.D. Thesis, Cybersecurity, California State University, San Marcos, CA, USA, 2022.
21. Guan, J.; Huck, J. Children in the digital age: exploring issues of cybersecurity. In Proceedings of the 2012 iConference, Toronto, ON, Canada, 7–10 February 2012; ACM: Toronto, ON, Canada, 2012; pp. 506–507. [CrossRef]
22. Anon. Exploring UK Parent Cyber Responsibilisation. *GIQ* 2023, *under review*.
23. Muir, K.; Joinson, A. An exploratory study into the negotiation of cyber-security within the family home. *Front. Psychol.* **2020**, *11*, 424. [CrossRef]
24. Office for National Statistics. Trust in Government, UK: 2022. 2022. Available online: https://www.ons.gov.uk/peoplepopulationandcommunity/wellbeing/bulletins/trustingovernmentuk/2022 (accessed on 4 April 2023).
25. Edelman. 2023 Edelman Trust Barometer. 2023. Available online: https://edl.mn/3X0QXQE (accessed on 1 June 2023).
26. Renaud, K.; van de Schyff, K.; MacDonald, S. Would US citizens accept cybersecurity deresponsibilization? Perhaps not. *Comput. Secur.* **2023**, *2023*, 103301. [CrossRef]
27. Shamir, R. The age of responsibilization: On market-embedded morality. *Econ. Soc.* **2008**, *37*, 1–19. [CrossRef]
28. Pellandini-Simányi, L.; Conte, L. Consumer de-responsibilization: changing notions of consumer subjects and market moralities after the 2008–2009 financial crisis. *Consum. Mark. Cult.* **2021**, *24*, 280–305. [CrossRef]
29. Ahmad, N.; Asma'Mokhtar, U.; Fauzi, W.F.P.; Othman, Z.A.; Yeop, Y.H.; Abdullah, S.N.H.S. Cyber security situational awareness among parents. In Proceedings of the 2018 Cyber Resilience Conference (CRC), Utrajava, Malaysia, 13–15 November 2018; pp. 1–3. [CrossRef]

30. Prior, S.; Renaud, K. The impact of financial deprivation on children's cybersecurity knowledge & abilities. *Educ. Inf. Technol.* **2022**, *27*, 10563–10583. [CrossRef]
31. Rahman, N.A.A.; Sairi, I.; Zizi, N.; Khalid, F. The importance of cybersecurity education in school. *Int. J. Inf. Educ. Technol.* **2020**, *10*, 378–382. [CrossRef]
32. Sağlam, R.B.; Miller, V.; Franqueira, V.N. A Systematic Literature Review on Cyber Security Education for Children. *IEEE Trans. Educ.* **2023**, *66*, 274 – 286. [CrossRef]
33. Quayyum, F. Cyber security education for children through gamification: Challenges and research perspectives. In Proceedings of the 10th International Conference on Methodologies and Intelligent Systems for Technology Enhanced Learning, L'Aquila, Italy, 16–19 June 2020; Workshops: Volume 2; Kubincová, Z., Lancia, L., Popescu, E., Nakayama, M., Scarano, V., Gil, A., Eds.; Springer International Publishing: Berlin, Germany, 2021; pp. 258–263. [CrossRef]
34. Amankwa, E. Relevance of Cybersecurity Education at Pedagogy Levels in Schools. *J. Inf. Secur.* **2021**, *12*, 233–249. [CrossRef]
35. Chiou, Y.M.; Shen, C.C.; Mouza, C.; Rutherford, T. Augmented reality-based cybersecurity education on phishing. In Proceedings of the International Conference on Artificial Intelligence and Virtual Reality (AIVR), Taichung, Taiwan, 15–17 November 2021; pp. 228–231. [CrossRef]
36. Yuliana, Y. The importance of cybersecurity awareness for children. *Lampung J. Int. Law* **2022**, *4*, 41–48. [CrossRef]
37. Nicholson, J.; Terry, J.; Beckett, H.; Kumar, P. Understanding Young People's Experiences of Cybersecurity. In Proceedings of the EuroUSEC'21: Proceedings of the 2021 European Symposium on Usable Security, Online, 11–12 October 2021; pp. 200–210. [CrossRef]
38. Lamond, M.; Renaud, K.; Wood, L.; Prior, S. SOK: young children's cybersecurity knowledge and skills. In Proceedings of the EuroUSEC, Karlsruhe, Germany, 29–30 September 2022; pp. 14–27. [CrossRef]
39. National Cyber Security Centre. Create Your Cyber Action Plan. 2022. Available online: https://www.ncsc.gov.uk/cyberaware/actionplan (accessed on 1 September 2022).
40. Nicholson, J.; Coventry, L.; Briggs, P. Introducing the Cybersurvival Task: Assessing and Addressing Staff Beliefs about Effective Cyber Protection. In Proceedings of the Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018), Baltimore, MD, USA, 12–14 August 2018; pp. 443–457.
41. Ondrušková, D.; Pospíšil, R. The good practices for implementation of cyber security education for school children. *Contemp. Educ. Technol.* **2023**, *15*, ep435. [CrossRef]
42. Chrispeels, J. Effective schools and home-school-community partnership roles: A framework for parent involvement. *Sch. Eff. Sch. Improv.* **1996**, *7*, 297–323. [CrossRef]
43. Quayyum, F. Collaboration between parents and children to raise cybersecurity awareness. In Proceedings of the European Interdisciplinary Cybersecurity Conference, Stavanger, Norway, 14–15 June 2023; pp. 149–152. [CrossRef]
44. Clark, A. *Cybersecurity in the UK*; House of Commons Library: London, UK, 2023.
45. Prior, S.; Renaud, K. Age-appropriate password "best practice" ontologies for early educators and parents. *Int. J. Child-Comput. Interact.* **2020**, *23–24*, 100169. [CrossRef]
46. Renaud, K.; Prior, S. Children's password-related books: efficacious, vexatious and incongruous. *Early Child. Educ. J.* **2021**, *49*, 387–400. [CrossRef]
47. Rawlings, R. Password Habits in the US and the UK: This Is What We Found. 2020. Available online: https://nordpass.com/blog/password-habits-statistics/ (accessed on 24 June 2023).
48. Özer, Ö.; Subramanian, U.; Wang, Y. Information sharing, advice provision, or delegation: What leads to higher trust and trustworthiness? *Manag. Sci.* **2018**, *64*, 474–493. [CrossRef]
49. Redmiles, E.M.; Malone, A.R.; Mazurek, M.L. I think they're trying to tell me something: Advice sources and selection for digital security. In Proceedings of the IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 22–26 May 2016; pp. 272–288. [CrossRef]
50. Marques, J.F. Unlearning: The hardest lesson of all. *Perform. Improv.* **2007**, *46*, 5–6. [CrossRef]
51. Liebowitz, S.J.; Margolis, S.E. Path dependence, lock-in, and history. *J. Law Econ. Organ.* **1995**, *11*, 205–226. [CrossRef]
52. Jennings, W.; Stoker, G.; Valgarðsson, V.; Devine, D.; Gaskell, J. How trust, mistrust and distrust shape the governance of the COVID-19 crisis. *J. Eur. Public Policy* **2021**, *28*, 1174–1196. [CrossRef]
53. Meredith, S. UK Prime Minister Boris Johnson Resigns. 2022. Available online: https://www.cnbc.com/2022/07/07/boris-johnson-resigns-as-uk-prime-minister.html (accessed on 1 August 2022).
54. Davies, B.; Lalot, F.; Peitz, L.; Heering, M.S.; Ozkececi, H.; Babaian, J.; Davies Hayon, K.; Broadwood, J.; Abrams, D. Changes in political trust in Britain during the COVID-19 pandemic in 2020: integrated public opinion evidence and implications. *Humanit. Soc. Sci. Commun.* **2021**, *8*, 166. [CrossRef]
55. Solly, B. In Teachers We (Absolutely Must) Trust.... 2021. Available online: https://www.sec-ed.co.uk/best-practice/in-teachers-we-absolutely-must-trust-school-improvement-retention-teaching-learning-pedagogy-accountability-leadership/ (accessed on 4 February 2023).
56. Mori, I. Ipsos Veracity Index. 2022. Available online: https://www.ipsos.com/en-uk/ipsos-veracity-index-2022 (accessed on 5 April 2023).
57. Pusey, P.; Sadera, W.A. Cyberethics, cybersafety, and cybersecurity: Preservice teacher knowledge, preparedness, and the need for teacher education to make a difference. *J. Digit. Learn. Teach. Educ.* **2011**, *28*, 82–85. [CrossRef]

58. Pusey, P.; Sadera, W. Preservice teacher concerns about teaching cyberethics, cybersafety, and cybersecurity: A focus group study. In Proceedings of the Society for Information Technology & Teacher Education International Conference, Austin, TX, USA, 5–9 March 2012; pp. 3415–3419.
59. Weale, S. UK Teachers 'Popping Pills' as Workload Grinds Them Down, Union Told. 2022. Available online: https://www.theguardian.com/education/2022/apr/16/uk-teachers-popping-pills-workload-grinds-down-union-nasuwt (accessed on 14 September 2022).
60. National Literacy Trust. Book Ownership in 2022. 2022. Available online: https://literacytrust.org.uk/research-services/research-reports/book-ownership-in-2022/ (accessed on 15 October 2022).
61. Starbuck, L. Camilla and Kate Join Forces to Get Children Reading. 2022. Available online: https://royalcentral.co.uk/uk/camilla-and-kate-join-forces-to-get-children-reading-173402/ (accessed on 15 October 2022).
62. Parr, C. People Trust Academics Far More than They Did in the 1990s. 2019. Available online: https://www.researchprofessionalnews.com/rr-news-uk-careers-2019-11-people-trust-academics-far-more-than-they-did-in-the-1990s/ (accessed on 22 November 2022).
63. Radrizzani, S.; Fonseca, C.; Woollard, A.; Pettitt, J.; Hurst, L.D. Both trust in, and polarization of trust in, relevant sciences have increased through the COVID-19 pandemic. *PLoS ONE* **2023**, *18*, e0278169. [CrossRef]
64. The British Academy. Academics Top 'Trust' List in British Academy Poll. 2022. Available online: https://www.thebritishacademy.ac.uk/news/academics-top-trust-list-in-british-academy-poll/ (accessed on 3 February 2023).
65. Al-Naser, A.E.; Bushager, A.; Al-Junaid, H. Parents' awareness and readiness for smart devices' cybersecurity. In Proceedings of the 2nd Smart Cities Symposium (SCS 2019), Manama, Bahrain, 24–26 March 2019; pp. 1–7. [CrossRef]
66. Google. How Google Fights Disinformation. 2019. Available online: https://www.blog.google/documents/37/How_Google_Fights_Disinformation.pdf (accessed on 17 January 2023).
67. National Cyber Security Centre. Advice on How to Stay Secure Online from the UK's National Cyber Security Centre. 2022. Available online: https://www.ncsc.gov.uk/cyberaware/home (accessed on 1 September 2022).
68. BBC. The Official Home of CBBC-CBBC-BBC. 2022. Available online: https://www.bbc.co.uk/cbbc (accessed on 1 August 2022).
69. Chartered Society of Physiotherapy. Thinking Differently about Support Workers. 2020. Available online: https://www.csp.org.uk/networks/associates-support-workers/thinking-differently-about-support-workers (accessed on 1 June 2023).
70. Skills for Schools. Parent Support Adviser, Undated. Available online: http://www.skillsforschools.org.uk/roles-in-schools/parent-support-adviser/ (accessed on 1 September 2022).
71. Stewart, C. Teaching Union Warns of Staffing Issues in Scottish Schools. 2023. Available online: https://www.heraldscotland.com/business_hq/23550569.teaching-union-warns-staffing-issues-scottish-schools/ (accessed on 1 June 2023).
72. GOV.UK. Government Cyber Security Strategy: 2022 to 2030. 2022. Available online: https://www.gov.uk/government/publications/government-cyber-security-strategy-2022-to-2030 (accessed on 6 May 2023).
73. Skipp, A.; Hopwood, V. Deployment of Teaching Assistants in Schools. 2019. Available online: https://www.gov.uk/government/publications/the-deployment-of-teaching-assistants-in-schools (accessed on 1 June 2023).
74. Robinson, J. Northumberland Youth Clubs Could Be Forced to Turn Children Away after Council Cuts 12 Jobs. 2023. Available online: https://www.chroniclelive.co.uk/news/north-east-news/northumberland-youth-clubs-could-forced-27170272 (accessed on 1 June 2023).
75. Ricci, J.; Breitinger, F.; Baggili, I. Survey results on adults and cybersecurity education. *Educ. Inf. Technol.* **2019**, *24*, 231–249. [CrossRef]
76. Federal Bureau of Investigation. Internet Crime Report 2020. 2020. Available online: https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf (accessed on 1 June 2023).
77. Stephenson, W. Correlating Persons Instead of Tests. *J. Personal.* **1935**, *4*, 17–24. [CrossRef]
78. R. Brown, S. A Primer on Q Methodology. *Operant. Subj.* **1993**, *16*, 91–138. [CrossRef]
79. Watts, S.; Stenner, P. Doing Q methodology: theory, method and interpretation. *Qual. Res. Psychol.* **2005**, *2*, 67–91. [CrossRef]
80. Nicholson, J.; Coventry, L.; Briggs, P. "If It's Important It Will Be A Headline" Cybersecurity Information Seeking in Older Adults. In Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, Glasgow, UK, 4–9 May 2019; pp. 1–11. [CrossRef]
81. Bada, M.; Sasse, A.M.; Nurse, J.R. Cyber security awareness campaigns: Why do they fail to change behaviour? *arXiv* **2019**, arXiv:1901.02672.
82. Watson, H.; Moju-Igbene, E.; Kumari, A.; Das, S. "We Hold Each Other Accountable": Unpacking How Social Groups Approach Cybersecurity and Privacy Together. In Proceedings of the CHI Conference on Human Factors in Computing Systems, Online, 25–30 April 2020; pp. 1–12. [CrossRef]
83. Turner, S.; Pattnaik, N.; Nurse, J.R.; Li, S. "You Just Assume It Is In There, I Guess": Understanding UK Families' Application and Knowledge of Smart Home Cyber Security. *Proc. ACM Hum.-Comput. Interact.* **2022**, *6*, 1–34. [CrossRef]
84. Wallace, S.; Green, K.; Johnson, C.; Cooper, J.; Gilstrap, C. An Extended TOE Framework for Cybersecurity Adoption Decisions. *Commun. Assoc. Inf. Syst.* **2021**, *47*, 51. [CrossRef]
85. Tazi, F.; Shrestha, S.; Norton, D.; Walsh, K.; Das, S. Parents, educators, & caregivers cybersecurity & privacy concerns for remote learning during COVID-19. In Proceedings of the CHI Greece 2021: 1st International Conference of the ACM Greek SIGCHI Chapter, Online, 25–27 November 2021; pp. 1–5.

86. Quayyum, F.; Bueie, J.; Cruzes, D.S.; Jaccheri, L.; Vidal, J.C.T. Understanding parents' perceptions of children's cybersecurity awareness in Norway. In Proceedings of the Conference on Information Technology for Social Good, Rome, Italy, 9–11 September 2021; pp. 236–241. [CrossRef]
87. AlShabibi, A.; Al-Suqri, M. Cybersecurity awareness and its impact on protecting children in cyberspace. In Proceedings of the 22nd International Arab Conference on Information Technology (ACIT), Ajman, United Arab Emirates, 22–24 November 2021; pp. 1–6. [CrossRef]
88. Milkaite, I.; Lievens, E. The internet of toys: playing games with children's data? In *The Internet of Toys: Practices, Affordances and the Political Economy of Children'S Smart Play*; Mascheroni, G., Holloway, D., Eds.; Springer: Cham, Switzerland, 2019; pp. 285–305. [CrossRef]
89. Halevi, T.; Memon, N.; Lewis, J.; Kumaraguru, P.; Arora, S.; Dagar, N.; Aloul, F.; Chen, J. Cultural and psychological factors in cyber-security. In Proceedings of the 18th International Conference on Information Integration and Web-Based Applications and Services, Singapore, 28–30 November 2016; pp. 318–324. [CrossRef]
90. Odebade, A.T.; Benkhelifa, E. Evaluating the impact of government Cyber Security initiatives in the UK. *arXiv* **2023**, arXiv:2303.13943.
91. UK Parliament. Online Safety Bill: HL Bill 87 of 2022–2023. 2023. Available online: https://lordslibrary.parliament.uk/research-briefings/lln-2023-0005/ (accessed on 1 May 2023).
92. Lepper, D. Cost-of-Living Crisis: The Challenges in 2023. 2023. Available online: https://charitydigital.org.uk/topics/topics/cost-of-living-crisis-the-challenges-in-2023-10678#:~:text=Cost-of-living (accessed on 1 June 2023).
93. Rose, R.; Wessels, B. Money, sex and broken promises: Politicians' bad behaviour reduces trust. *Parliam. Aff.* **2019**, *72*, 481–500. [CrossRef]
94. Grimmelikhuijsen, S.; Knies, E. Validating a scale for citizen trust in government organizations. *Int. Rev. Adm. Sci.* **2017**, *83*, 583–601. [CrossRef]
95. Bayrakdar, S.; Guveli, A. *Inequalities in Home Learning and Schools' Provision of Distance Teaching during School Closure of COVID-19 Lockdown in the UK*; Technical Report ISER Working Paper Series No. 2020-09; Institute for Social and Econmic Research: Colchester, UK, 2020. Available online: https://repository.essex.ac.uk/27995/ (accessed on 27 June 2023).